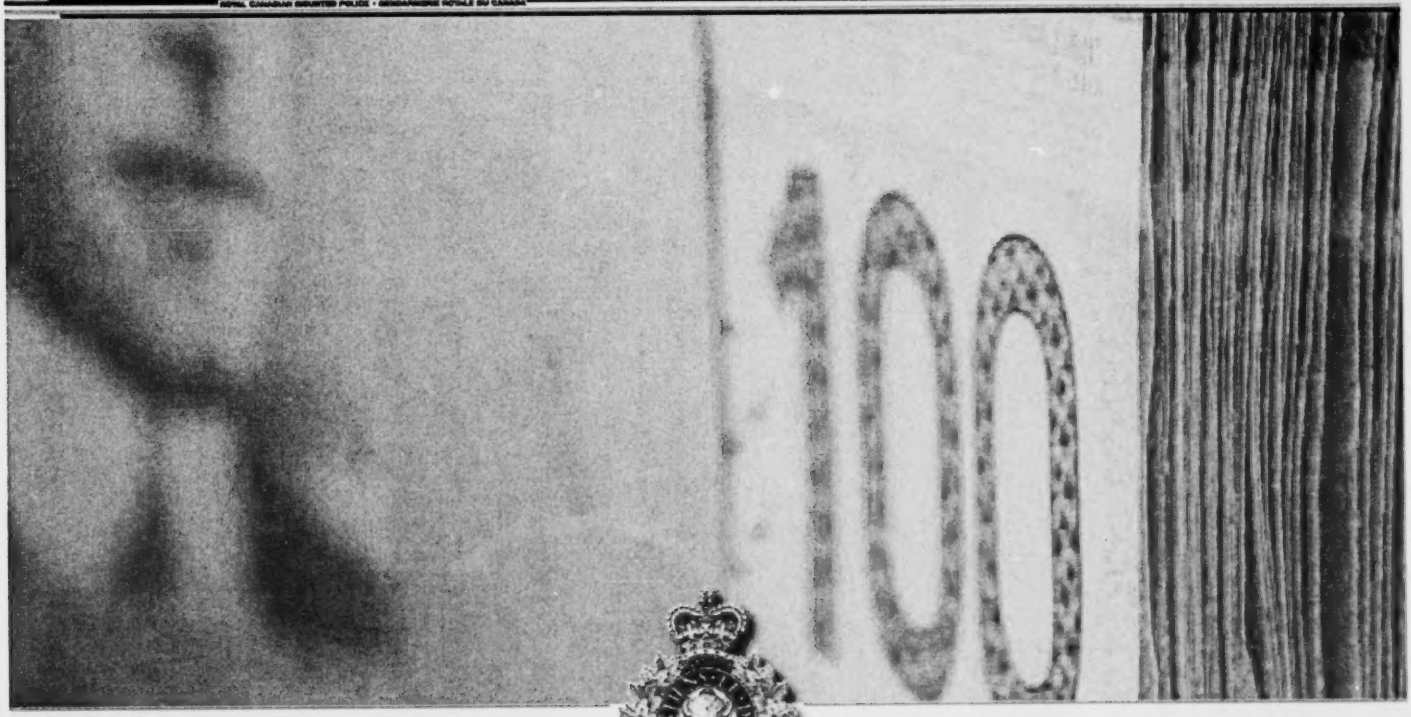
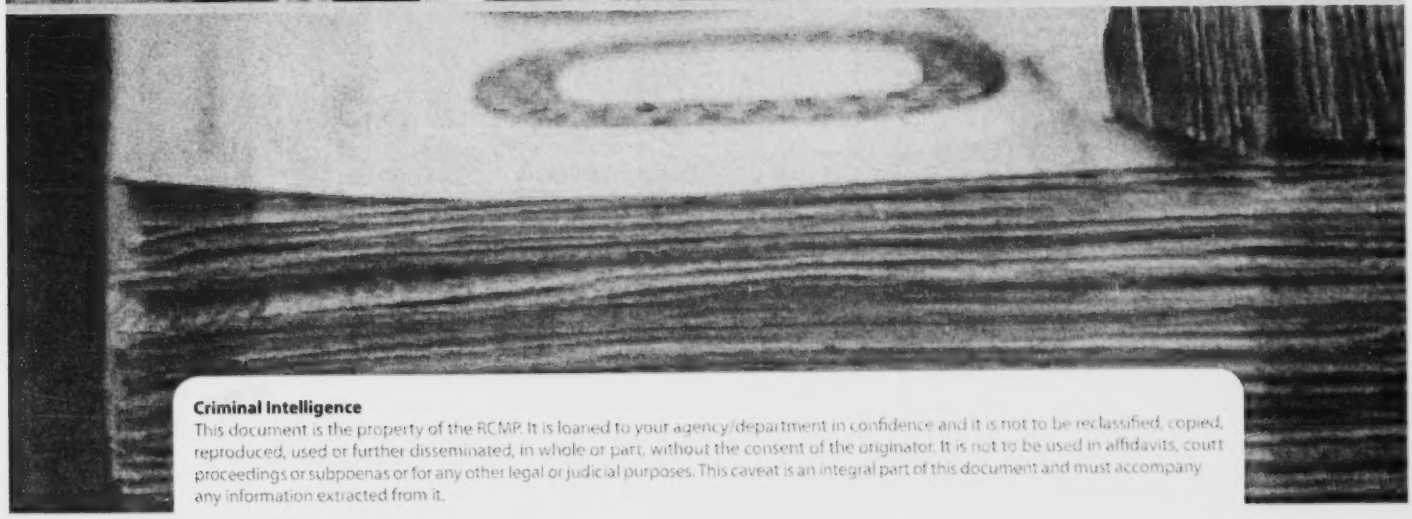


Threat Assessment: Mass-Marketing Fraud

The Canadian Perspective — Nov. 2007



FORWARD

This report was jointly prepared by the Royal Canadian Mounted Police (RCMP) Commercial Crime Branch and Criminal Intelligence.

The RCMP extends its appreciation to all Canadian and international partners who contributed to this threat assessment on mass-marketing fraud.

Collaboration on the part of the Canadian Anti-Fraud Call Centre (CAFCC), the members of the Canadian mass-marketing fraud enforcement partnerships and the National Mass Marketing Fraud Strategy Working Group was invaluable.

This threat assessment was initiated in support of the National Mass Marketing Fraud Strategy. This assessment will be used as the Canadian submission to Project STOP PAYMENT, a Joint International Threat Assessment on Mass Marketing Fraud.

Please address any inquiries regarding this assessment to:

Royal Canadian Mounted Police
Commercial Crime Branch
1200 Vanier Parkway
Ottawa, Ontario
Canada
K1A OR2

or

RoyalCanadian Mounted Police
Criminal Intelligence
1200 Vanier Parkway
Ottawa, Ontario
Canada
K1A OR2

Table of Contents

Table of Contents

EXECUTIVE SUMMARY

Over the past 10 to 15 years mass-marketing fraud (MMF) has proliferated. Criminals and criminal organizations are involved. In Canada, the majority of schemes documented are advance fee lottery, sweepstakes pitches with counterfeit cheques, credit card pitches, government grant and loan pitches, directory pitches, investment pitches, job offer schemes, and schemes involving sales of merchandise over the Internet.

MMF has been identified as a cross-border crime concern between Canada and the United States (U.S.) since 1997. Joint responses to MMF include the creation of six regionalized partnerships and the Canadian Anti-Fraud Call Centre (CAFCC), also known as PhoneBusters. All of these partnerships require coordination and cooperation amongst law enforcement and regulatory agencies at local, provincial, national and international levels.

Current Types of Criminal Activities

With advances in communication technologies, including the Internet, cell phones, electronic banking and wire transfers, the MMF problem has become international in nature and global in its scope. While mass-marketing fraud through mail and telephone remains an ongoing concern, fraud is increasingly committed through the Internet. Voice over Internet Protocol (VOIP) and prepaid cell phones have allowed for MMF operators to become more mobile, giving them the ability to operate from any location they choose, with any area code and phone number they want. This creates law enforcement challenges in identifying who the criminals are and where they are operating from.

Some criminal networks established in Canada are involved in international MMF scams and distribute counterfeit financial instruments across jurisdictions through mail and courier services.

Identity theft is an intricate part of MMF operations. Many of the fraudulent solicitation pitches induce potential victims into divulging their personal information to criminals and risking further victimization through identity fraud. Personal information from potential victims is used to facilitate ongoing schemes and produce lead lists. These lists are resold to other groups/rings to perpetrate other fraudulent crimes.

MMF is a lucrative business for criminals. In its 2006-2007 annual report, the Financial Transactions and Reports Analysis Centre of Canada, known as FINTRAC, reported that fraud-related predicate offences (e.g. credit and debit card fraud, and telemarketing fraud) were more prevalent than drug-related cases in 2006-07.

In Canada, crimes against persons, such as threats, intimidation and assaults against ex-employees, victims or witnesses, have been associated to MMF operations. Past investigations indicate that some MMF activities in Canada are subject to protection rackets.

Incidence and Prevalence of Criminal Activities

Between 2004 and 2006, CAFCC statistics indicate an increase in reported dollars loss for MMF complaints. Additionally, the number of telephone calls received at the centre increased by almost 60 percent, from 92,307 in 2005 to 146,393 in 2006.

Currently, the most common trend in MMF is the use of counterfeit or altered financial instruments (cheques/money orders). Between March and April 2007, nearly 30 percent of complaints received at CAFCC involved the use of a counterfeit financial instrument. Schemes documented that involve counterfeit cheques are global in nature, often using foreign bank accounts to facilitate money laundering.

Canadian-based MMF operations mostly target citizens from Canada and the United States, and to a lesser degree, the United Kingdom and other English speaking countries. MMF operations outside Canada reported by Canadians are mainly based in the United States, the United Kingdom and Spain.

Ontario, Quebec, British Columbia and Alberta are the top-ranking MMF criminal locales in Canada, with Ontario accounting for almost half of the reported locations. The lottery, sweepstake, grants and loans, and credit card schemes are operated in all locales. Directory and office supply scams operate primarily from Montreal with some operations in Toronto. In 2006, 73.9 percent of the complaints received at CAFCC on Canadian suspects were received from consumers in other countries. Schemes originating in Canada primarily target U.S. citizens.

Canadians have reported being solicited with schemes originating from 105 different countries worldwide. Communication methods such as email, Voice over Internet Protocol (VoIP) and the Internet in general, are making it easier for criminals to communicate with their intended victims. The majority of complaints originated from the United States, followed by the United Kingdom, Spain and Nigeria.

Principal Techniques Used for Fraud

Facilitators of MMF activities, whether witting or unwitting, may be used by MMF operations in the various phases of their fraudulent operations, including the initial set up of a scam, the identification of potential vict[illegible], reaching and communicating with intended victims, receiving victim funds and laundering of proceeds. Facilitators vary depending on the size and level of sophistication of the scheme being run.

Overall in the last 3 years, telemarketing (direct call) has ranked the highest amongst solicitation methods in terms of the number of reported occurrence and is followed in order by mail, Internet, print, and in-person.

Receipt and Laundering of Mass-Marketing Fraud Proceeds

In the past, funds were mostly forwarded by victims to the fraudster by way of a cheque or cash through the mail stream. Now, money transfer businesses are increasingly used by fraudsters to receive funds from victims, mainly for money transfers involving transactions of less than $10,000. Cashier's cheques and bank-to-bank wire transfers are the most common methods for transactions involving amounts of $10,000 and above. In regards to fraudulent activities committed through the Internet as the primary means of communication and transaction, payments are usually received via Internet Payment Systems (IPS).

On the money laundering front, some of the current methods that have been used for some time are: "smurfing"[1] electronic funds transfer, the use of money service businesses, casinos, credit cards and co-mingling of funds using legitimate businesses. Furthermore, a few emerging trends that are particularly of interest to the laundering of proceeds obtained from mass marketing frauds are: money laundering through Internet Payment Systems (IPS), prepaid credit cards and digital currencies.

Several cases investigated in Canada show that mass-marketing fraud operations can generate substantial amounts of revenues in a relatively short period of time. For example, in Montreal, Project Coral[2] unveiled a criminal operation which generated over $30 million U.S. in 18 months. In a case investigated by Project EMPTOR, an RCMP-led Task Force in British Columbia, a fraudulent scheme operated by a British Columbia couple, involving selling credit card protection to customers across the United States, took in more than $10 million from thousands of victims.

1 Money laundering technique consisting of making deposits just below the reporting threshold in various bank accounts housed in multiple banks

2 Project Coral – See case summary in Part "G" under "Enforcement" sub-heading.

Current "Best Practices" for Reducing Incidence and Prevalence of Mass-Marketing Fraud

Today, PhoneBusters is known as The Canadian Anti-Fraud Call Centre (CAFCC) and plays a key role in education and prevention of mass marketing fraud schemes while promoting the principles of intelligence-led policing through the collection, analysis and dissemination of complaint and victim information to law enforcement agencies. Centralization of fraud complaints is a key element to enabling better information sharing and intelligence.

In Canada, the six MMF partnerships, which include three co-located task forces in Montreal, Toronto and Vancouver, are the main enforcement bodies that investigate, disrupt and dismantle MMF operations. Many MMF cross-border cases between Canada and the United States have been successfully investigated and prosecuted since 1998.

March is Fraud Prevention Month in Canada and around the world. During the month, Fraud Prevention Forum members raise awareness of the dangers of fraud, while educating the public on how to: *"Recognize it. Report it. Stop it."*

Conclusion

Mass-marketing fraud remains a problem in Canada and is causing severe harm to Canadians and foreigners alike. While mass-marketing fraud operations continue in Canada, similar operations in other countries grow. MMF is perceived by criminals as a high-profit, low risk criminal activity and has become an attractive venture for organized crime groups.

In Canada the top schemes, in order, are: prize (including lottery and sweepstakes) pitches, the work at home/ job opportunities, foreign money offers (419 scams), loan pitches and overpayment (sale of merchandise) scams. In recent years, all of these have been associated to the use of counterfeit or altered monetary instruments and all are international in scope.

INTRODUCTION

Over the past 10 to 15 years mass-marketing fraud (MMF) has proliferated. This proliferation is not only in the number of MMF offences or attempts, but also in the number and nature of activities. The MMF problem now appears to be international in nature and global in its scope. Criminals and criminal organizations are involved. Several countries have identified MMF activities as an enforcement problem and have recognized the need for a coordinated enforcement approach.

With more advanced methods of communication available, criminals are capable of reaching far greater audiences, at far greater distances.

MMF came to the attention of law enforcement in the early 1990's and has been identified as a significant economic crime problem in Canada, and a cross-border crime concern between Canada and the United States (U.S.) since 1997. From 1993 to 2006 there were a number of joint responses to MMF including the creation of six regionalized partnerships and the Canadian Anti-Fraud Call Centre (CAFCC), previously known as PhoneBusters. All of these required coordination and cooperation amongst law enforcement and regulatory agencies at local, provincial, national and international levels.

MMF activities occurring in Canada impact Canadians and citizens of other countries and are committed by individuals acting alone and by organized groups. Some criminals involved in MMF are likely to be repeat offenders and some victims are likely to be repeat victims.

Not all MMF occurring in Canada targets Canadians and not all criminals engaged in MMF in Canada are Canadian citizens. This report will not identify the modus operandi of all schemes nor can it identify all groups involved.

MMF criminals take advantage of communication technology to mask the locations from which they operate, and to increase the scope of their activities at reduced costs. Jurisdictional issues affect the public, police and other government agencies.

Investigators indicate that the largest deterrent to MMF offences operating in Canada is the possibility of being extradited to the United States, where jail terms could triple.

A. Historical Perspective — The Response to MMF

In 1993, the Ontario Provincial Police (OPP) initiated Project PhoneBusters in response to reported incidents of telemarketing fraud targeting Ontario residents. This project identified that telemarketing fraud was not only affecting consumers from Ontario, but consumers from across Canada and the United States. Between 1993 and 1996, through Project PhoneBusters enforcement activities, telemarketing fraud was identified as a growing crime concern in Canada and it gained the attention of both national and international law enforcement agencies.

A 1997 meeting between former President Clinton and former Prime Minister Chrétien on cross-border crime issues saw the establishment of a Bi-national Working Group on Cross Border Telemarketing Fraud. This Working Group, which became a sub-group to the Canada/U.S. Cross Border Crime Forum (CBCF), sought to "examine ways to counter the serious and growing problems of cross-border telemarketing fraud." This sub-committee recognized telemarketing fraud as a "serious and expanding problem" and identified a number of trends and activities taking place on both sides of the border[3].

1998 saw the creation of two RCMP-led task forces in Canadian hotbeds for fraudulent telemarketing operations. Project COLT was formed in Montreal and Project EMPTOR in Vancouver. Both are joint efforts involving law enforcement and regulatory agencies from the United States and Canada, and are mandated to investigate and prosecute Canadian-based MMF operators.

In 1999, the Federal Bureau of Investigation launched Operation Canadian Eagle. This operation enhanced cross-border coordination and cooperation in these task forces by assigning special agents to work directly with them.

By 1999, the Competition Act of Canada was amended to include an entire section on deceptive telemarketing.

In 2000, the Toronto Strategic Partnership was formed by law enforcement and regulatory agencies from both Canada and United States.

In 2001, the RCMP officially became a partner in PhoneBusters and it came to be known as PhoneBusters National Call Centre (PNCC). In 2002, PNCC expanded its operation to include an analytical unit with intelligence resources.

In 2003, the CBCF Subgroup on Mass Marketing Fraud released a five year report on MMF activities, identifying current trends relating to MMF. The report highlighted that between 1997 and 2002, cross-border fraud had increased substantially. The report detailed an action plan for the current challenges in cross-border fraud, calling it "the end of the beginning".[4]

The group found that cross-border telemarketing fraud had increased substantially from 1997 to 2002 in the areas of fraudulent prize schemes, lottery schemes, loan schemes, and in credit card protection and low interest credit card schemes. The report further identified the growing involvement of organized crime groups in Canadian-

3 http://www.usdoj.gov/criminal/fraud/uscwgrtf.htm (Report of the United States – Canada Working Group, United States – Canada Cooperation Against Cross-Border Telemarketing Fraud, November 1997.)

4 http://www.psepc-sppcc.gc.ca/prg/le/bs/massmfr-en.asp (Bi-national Working Group on Cross-Border Mass-Marketing Fraud, A Report to the Attorney General of the United States and the Solicitor General of Canada, May 2003.)

based telemarketing fraud operations. Other findings of this report include: identifying that "Internet-related cross-border fraud complaints have been steadily increasing in the past three years"; that "U.S. and Canadian data show that identity theft has become one of the fastest growing forms of crime", and; that "Africa-related fraud schemes...have been a longstanding problem for law enforcement in Canada, the United States and the United Kingdom."

In 2004, the Fraud Prevention Forum (FPF) was formed. The FPF is a concerned group of private sector firms, consumer and volunteer groups, government agencies and law enforcement organizations who are committed to fighting fraud aimed at consumers and businesses. Through its partners, the Forum, which is chaired by the Competition Bureau, works to prevent Canadians from becoming victims of fraud by educating them how to *"recognize it, report it, and stop it."*[5]

Between 2003 and 2005 three new partnerships were formed in Canada to continue and improve Canadian and U.S. partnerships combating MMF and to build on existing partnership successes. Also during this period, MMF operations began to appear outside previously identified locales.

These partnerships are known as the Alberta Partnership against Cross-Border Fraud, the Vancouver Strategic Alliance and the Atlantic Partnership Combating Cross-Border Fraud.

Between March 2005 and May 2006, the RCMP and its law enforcement partners took part in Operation Global Con. This action involved cooperation and coordination by law enforcement agencies at the national and international levels to target mass marketing schemes that were international in scope. In Canada alone 372 charges were laid.

In 2005, the National Mass Marketing Fraud Working Group (NMMFWG) was formed through informal and formal meetings held during late 2004 and part of 2005. By May 2006 the NMMFWG developed the National MMF Strategy with a goal to dismantle, disrupt, and neutralize Canadian-based MMF operations. To accomplish this goal the NMMFWG identified three core strategic objectives: increasing the business risk and cost for MMF operators, strengthening law enforcement effectiveness and decreasing victim susceptibility. The strategic framework is based on four pillars: 1) More vigorous enforcement; 2) Raised awareness; 3) Judicial impact; 4) Improved national data. The MMFWG is seeking to achieve the objectives through several initiatives over a period of three years, using existing and available resources.

5 http://www.competitionbureau.gc.ca/internet/index.cfm?itemID=2281&lg=e

B. Current Types of Criminal Activities

Telemarketing fraud, Internet fraud and mass-mailing fraud

Over the past decade, the response to MMF by law enforcement in Canada was based extensively on telemarketing fraud being identified as a cross-border crime problem between Canada and the United States. Numerous joint efforts between Canada and the United States have been undertaken to combat fraudulent telemarketing operations based in Canada.

Although most of us welcome emerging technologies which make our life easier, organized crime will take advantage of every new technology coming onto the market and any new business opportunity to expand their illegal activities. The advent of the Internet has certainly facilitated fraud schemes as hundreds of millions of web users can be reached and enticed by fraud artists. While mass-marketing fraud through mail and telephone remains an ongoing concern, fraud is increasingly facilitated through the Internet.

MMF scams now involve the extensive use of counterfeit financial instruments. In the last three years (2004-2006), CAFCC has documented an increase in the overall number of reported MMF incidents in all provinces except for Manitoba, Northwest Territories, Nunavut and Ontario. This increase can be explained by the use of counterfeit financial instruments (cheques, money orders) and the use of Internet by MMF operators in a number of scams, including advance fee schemes (lottery, sweepstakes, loan, credit card ,job offer, West-African 419), as well as overpayment schemes (sale of merchandise or renting property). In the past year, thirty percent (30%) of all complaints reported to the CAFCC involved the use of counterfeit cheques or money orders.

Identity theft related to MMF

The theft of personal and financial information and the fraudulent use of that data are facilitating mass-marketing fraud activity.

Documented complaints at CAFCC indicate MMF involvement in fraudulent, deceptive or misleading schemes specifically aimed at obtaining personal and financial data from unsuspecting victims. Many of the fraudulent solicitation pitches induce potential victims into divulging their personal information to criminals, and risking further victimization through identity fraud.

Once obtained, the data is used to create telemarketing lead or "sucker" lists from which fraudulent scams are committed. These lists are also resold to other criminal groups to perpetrate other fraudulent crimes.

Identity theft scams are undertaken by the use of a variety of sophisticated schemes designed to mislead, deceive or defraud unsuspecting citizens in countries around the world. Scammers use pressure tactics to lure victims into providing personal and banking information under a pretext, for example to become immediately eligible to win a prize.

The schemes are further enabled by the use of the Internet and by advances in technology. The Internet is being used to entice the unsuspecting public into revealing personal information. MMF suspects are also engaged in the use of malicious spyware, also designed to obtain personal information without the victims' knowledge.

MMF suspects also use the fraudulently obtained data for financial gain, to obtain goods and services or to facilitate anonymous travel. The data has been used to create fictitious identities or assume existing individual identities in order to rent vehicles or purchase airline tickets that enable national or international travel. Using this data, suspects are also able to submit fraudulent applications for consumer services such as cellular telephones, telephone connections, office lease, mail box rentals and bank accounts.

MMF suspects have also used the data to create fictitious sets of identity for use in the wire transfer of monies. This activity allows MMF operators to move funds around the world in anonymity, to pick up money from cash payment outlets.

Money Laundering

In its 2006-2007 annual report[6], the Financial Transactions and Reports Analysis Centre of Canada, known as FINTRAC, reported it made 193 disclosures about suspicious cases, totalling almost $10 billion, to police and security officials. What is interesting about this latest report however are the findings regarding trends and patterns: "In contrast to previous years, when most money laundering cases involved suspected drug-related offences, fraud-related predicate offences (e.g. credit and debit card fraud, **and telemarketing fraud**) were more prevalent in 2006-07".

In a 2007-10-25 press release, FINTRAC director Horst Intscher said: *"This year, for the first time, I'd say **fraud**-related cases are probably more numerous than the **drug**-related cases."* Intscher said many of these **fraud** files *"are as pernicious as any **drug**-related case_ targeting elderly people through **telemarketing** scams and phoney upfront payments for services never provided.* While in the past many cases involved drug trafficking proceeds, **fraud has become the biggest thread in questionable transactions.**

Threats, intimidation or violence

In Canada, crimes against persons, such as threats, intimidation, and assaults against ex-employees, victims or witnesses, have been associated to MMF operations. Often, reports from ex-employees document that boiler room operators would intimidate and threaten the employee not to report the activity. There is some evidence indicating that street gang members are becoming involved in MMF activities.

Canadian victims of foreign money scheme such as 419 letter fraud are sometimes enticed to travel to foreign countries where they risk further financial loss and even bodily harm. For example, in 2007, a Canadian man had fallen victim to an Internet "Lonely Heart" scam and had travelled to Ghana with the hope of meeting the women he had met on the Internet. He stayed in a hotel room in that country for several weeks. During that time he was defrauded of several thousand dollars. One of his neighbours in Canada, from whom he sought to borrow money, suspected he was an unwary victim, and reported the matter to the CAFCC. The man was subsequently located in Ghana by the RCMP Liaison Officer and was eventually rescued by the local police force. Intelligence received revealed that male suspects came by the hotel looking for the victim, only minutes after his departure.

Some MMF activities in Canada are subject to protection rackets, including biker gangs and traditional organised crime, with scam operators paying a percentage to operate in certain jurisdictions.

6 http://www.FINTRAC.gc.ca/publications/ar/2007/1-eng.asp

C. Incidence and Prevalence of Criminal Activities

The Proliferation of MMF in Canada

The very nature of mass marketing is to reach the largest potential market so as to maximize profit. When combined with the effects of globalization, and other influences such as the Internet and Voice over Internet Protocol (VoIP), mass marketing has no boundaries. As such, by its very nature, MMF is a global crime problem and we are now observing organizations, like the Organization for Economic Cooperation and Development and the International Consumer Protection and Enforcement Network, developing guidelines and working groups to specifically address the problem of MMF schemes.[7]

Mass-marketing fraud and related economic crimes are a very serious threat to our economy. These types of crimes can result in enormous financial losses for their victims which include governments, financial institutions, businesses and individuals. Victimization also results in a loss of confidence by the public in its institutions and processes, it undermines investor confidence and increases costs to the consumer.

Mass-marketing fraud complaints are currently gathered by law enforcement agencies across Canada, including the existing partnerships, as well as by the Competition Bureau and other provincial regulatory agencies. This makes attempts at determining the level or impact of MMF in Canada difficult.

Given these findings, and that all of the stakeholders are familiar with and make extensive use of CAFCC data, the majority of the reported data used for this assessment was drawn from the CAFCC and should only be considered a snapshot of the overall landscape of MMF in Canada.

For the purposes of this report, consumer complaint data and MMF information was obtained from a variety of public and police sources but relying primarily on data from the CAFCC to provide a snapshot of MMF in Canada.

Since data sources do not capture MMF complaints in a similar manner, it is not feasible to describe all of the various scheme types occurring. Furthermore, MMF schemes are flexible in nature; MMF operators can develop a different pitch for any product, service or event they choose. Their flexibility is demonstrated by the schemes that developed after tragic events such as the deaths of four RCMP members in Mayerthorpe, 9/11 and Hurricane Katrina. It was only a matter of days following these tragedies before schemes were developed to solicit funds using various charity themes.[8]

7 http://www.icpen.org/about.htm
http://www.oecd.org/document/53/0,2340,en_2649_34267_2516469_1_1_1_1,00.html

8 http://news.com.com/Online+scams+emerge+in+Katrinas+wake/2100-7349_3-5845695.html
http://www.cbsnews.com/stories/2005/09/09/katrina/main829212.shtml
http://www.rcmp-grc.gc.ca/ab/news/2005/Mayerthorpe_VictimFund_Apr11-05_NR17.htm

MMF schemes are financial crimes and are committed for profit. Albeit, schemes can vary in the level of sophistication and organization involved and some schemes solicit higher dollar amounts than others. Regardless, they are all serious frauds that impact Canada.

In terms of analyzing MMF from a Canadian perspective, two primary themes can be developed: Canadian-based MMF operations targeting Canadian and foreign victims, and Canadians being victimized by foreign-based MMF operations. Canadian-based MMF operations target mostly citizens from Canada and the United States, and to a lesser degree, the United Kingdom and other English speaking countries. MMF operations targeting Canadians from outside Canada, as reported by Canadians, are mainly based in the United States, the United Kingdom and Spain.

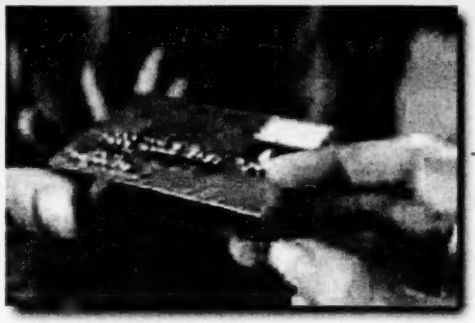
Between 2004 and 2006 CAFCC statistics indicate that the Canadian reported dollar loss for all MMF complaints increased from $19,174,234.48 to $25,916,962.36. Additionally, the number of telephone calls received at the centre increased by almost 60 percent, from 92,307 in 2005 to 146,393 in 2006.

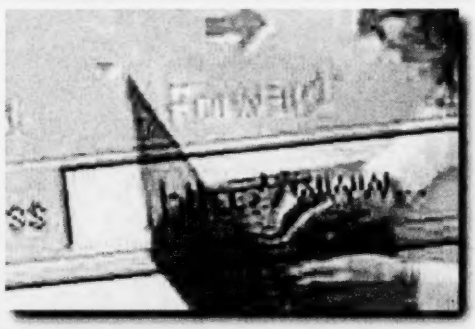
Table 1

	Phone Calls Received	Phone Calls Handled
2005	92,307	76,770
2006	146,393	104,002

Likewise, data from Consumer Sentinel and RECOL highlights that the number of reported incidents of MMF increased significantly from 2004 to 2006. RECOL reported receiving 3439 online complaints in 2004 and 5500 in 2006. Consumer Sentinel reported receiving 64,892 cross-border fraud complaints in 2004 and 95,249 in 2006.

MMF — Financial Crimes committed for profit



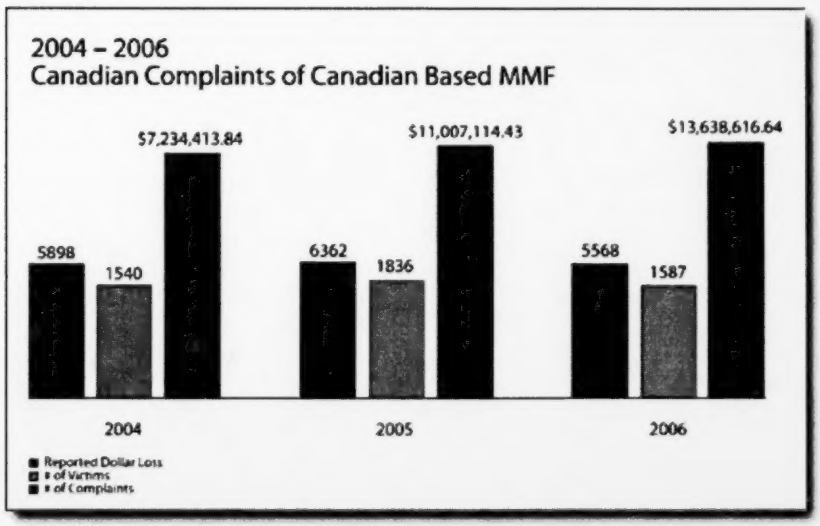


Canadians as Victims of Canadian-Based MMF

MMF operation locations are based on suspect addresses reported by consumers. Thus, it must be noted that in some cases, reported addresses may be mail drops and not the physical location of an MMF operation, or the suspect locations identified may be false. Finally, in some incidents, the consumer does not know or was never provided with a suspect address.

Canadians who report being solicited by Canadian-based MMF operations account for an average of 37.89 percent of the annual complaints received from 2004 to 2006, with the overall number of complaints remaining fairly constant. However, the reported dollar loss nearly doubles for the same time period (Chart 1).

Chart 1



The provincial breakdown for these figures is as follows (Chart 2-4)

Chart 2

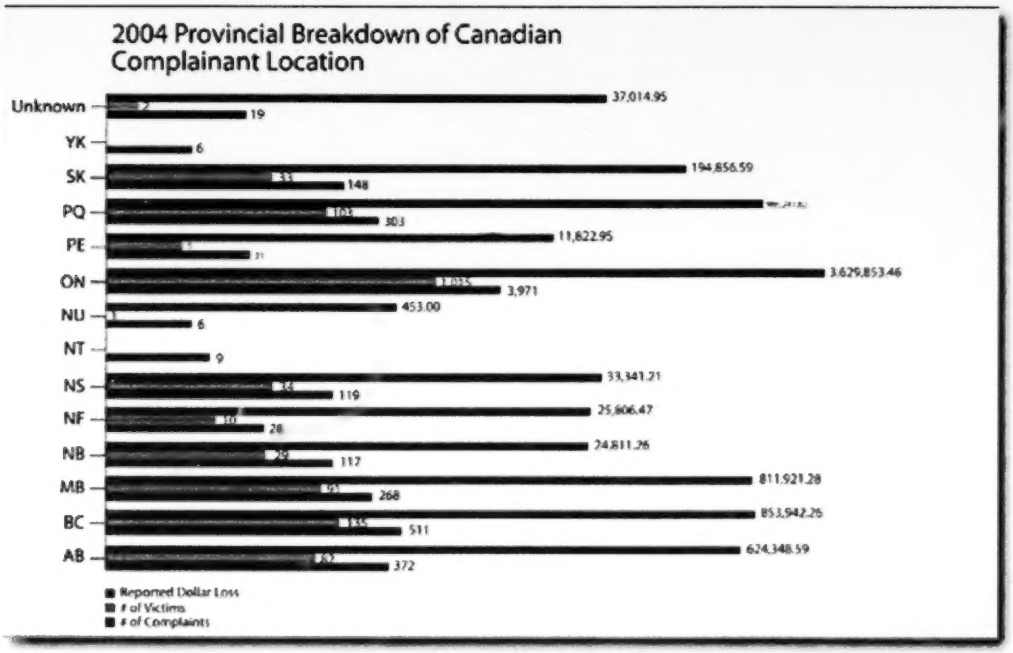


Chart 3

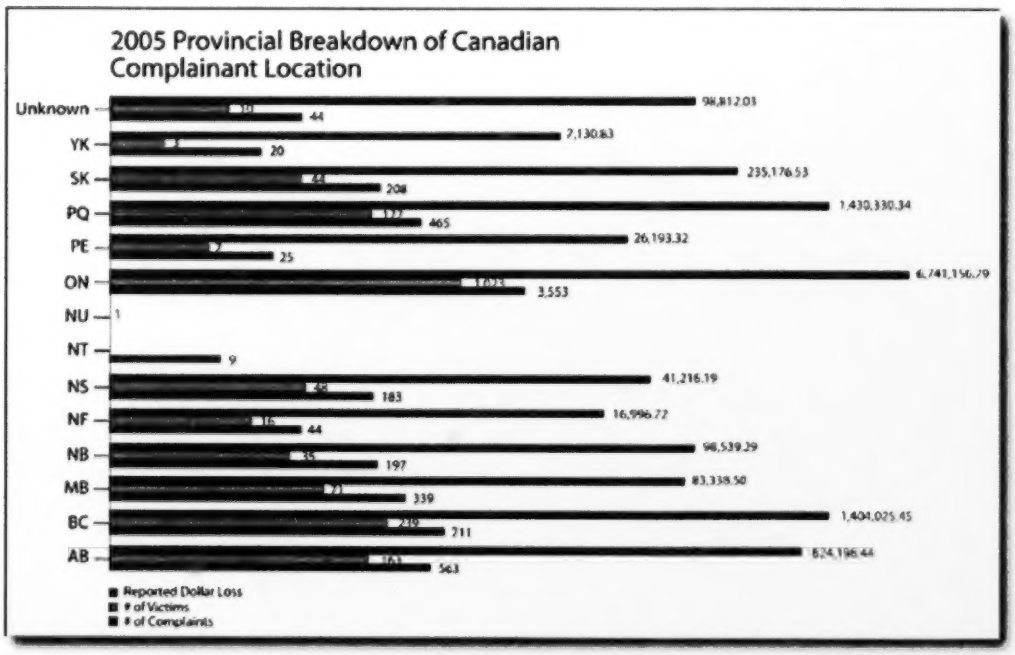
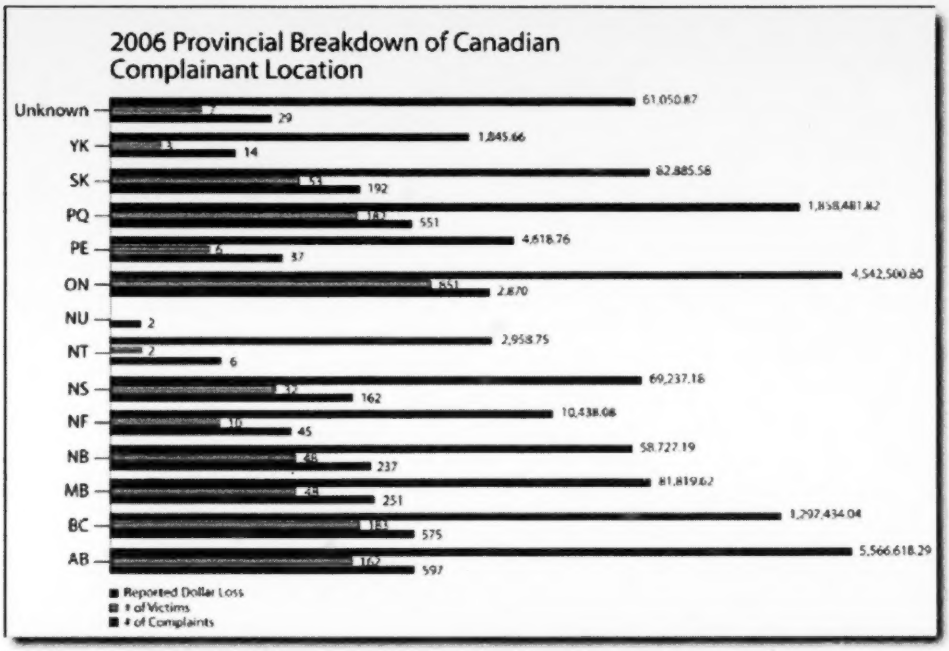


Chart 4



The above figures represent provincial reporting to CAFCC from 2004 to 2006. For this period, the top five provinces targeted by MMF schemes originating in Canada are Ontario, British Columbia, Quebec, Alberta, and Manitoba. Overall, the number of reported incidents increases in all provinces except for Manitoba, Northwest Territories, Nunavut and Ontario. Generally, CAFCC receives higher reporting rates from the more populous provinces.

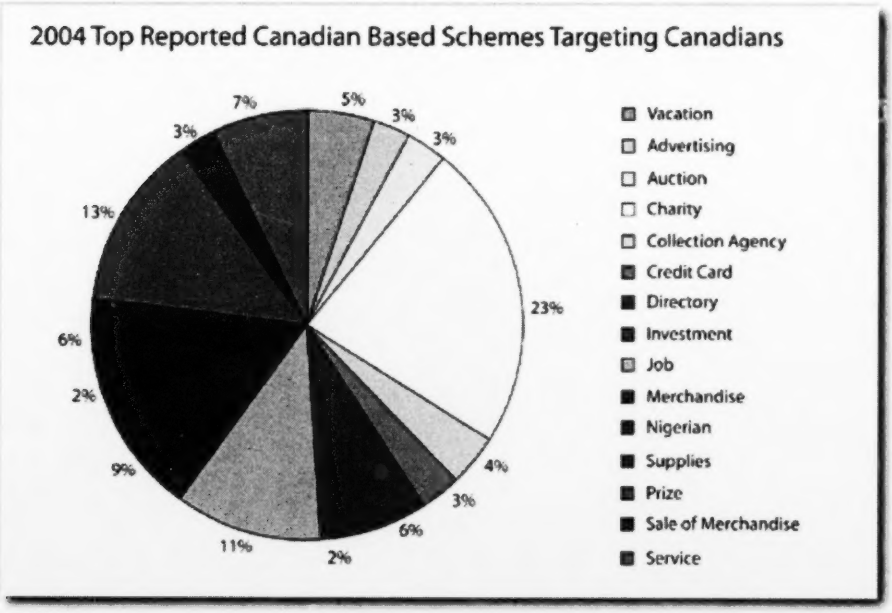
For the past 3 years, on average, reports from consumers in Ontario have made up 58.24 percent of the complaints received at CAFCC. This can be attributed to approximately one third of the Canadian population residing in Ontario and to the CAFCC being located in Ontario. Many of the educational initiatives conducted through CAFCC and SeniorBusters in the past have been concentrated on Ontario as the program was led by the Ontario Provincial Police. It is also important to highlight that from 2004 until 2006, the percentage of Ontario complaints dropped from 67.33 percent to 51.54 percent of the complaints. This can be attributed to greater educational efforts outside of the province undertaken through coordination by the FPF. Additionally, the study commissioned by the Competition Bureau in 2004 found that the name PhoneBusters was not widely known across Canada.

From 2004 to 2006, the top 15 schemes operated in Canada targeting Canadians are identified in the graphs below. Some of the most significant trends identified by the CAFCC Intelligence and Analytical Unit for this time frame include Canadians being victimized by loan schemes, and the increase in schemes being associated to traditional West-African 419 fraud. Loan schemes traditionally targeted American consumers through advertising in newspaper but have now shifted to solicitation through online ads and Internet sites.

While charity solicitations consistently rank as one of the top two for the past three consecutive years, the number of reported incidents significantly decreased in 2006. Contributors at CAFCC point out that many reports received regarding charities are from consumers inquiring about their legitimacy which does not necessarily identify them as MMF operations.

Increases in reported incidents were seen for prize, directory, service, office supplies, collection agencies, overpayment, investment and loan schemes. According to CAFCC Analytical Unit members, increases in the prize pitch and overpayment pitch can be associated to the use of counterfeit or altered financial instruments.[9] The increase in the loan pitch can be associated to use of the Internet to advertise loan scams.

Chart 5



9 Currently there is no database in Canada that can provide data on schemes involving counterfeit or altered financial instruments.

Chart 6

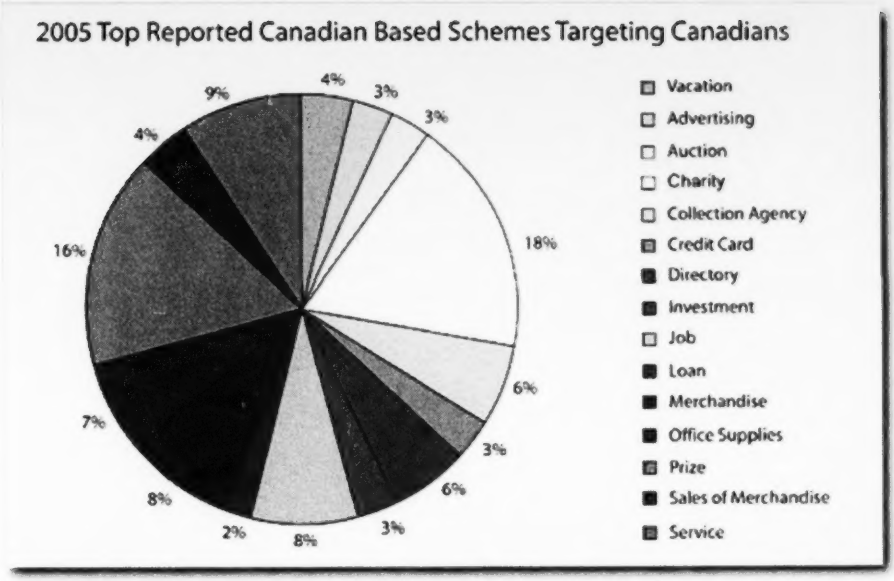
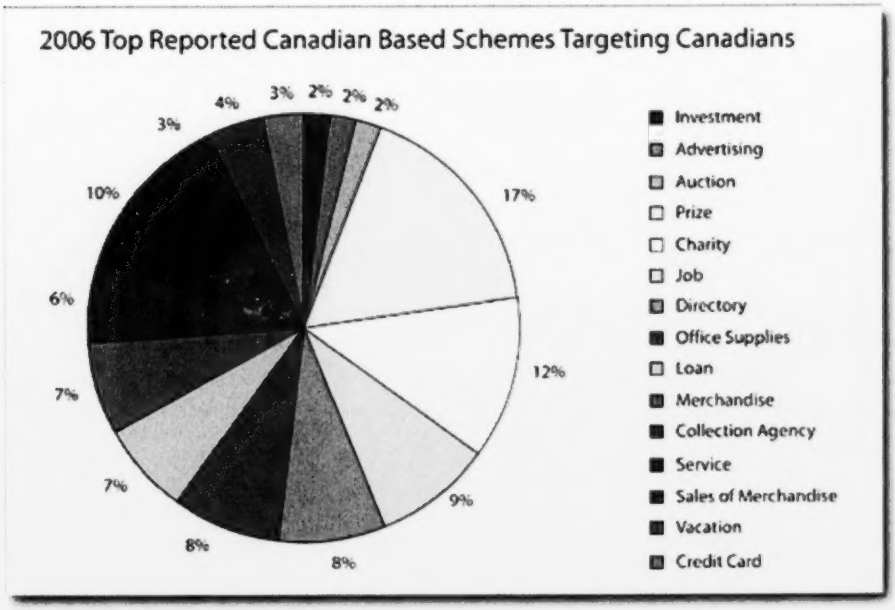


Chart 7



The following table represents the top scheme types reported to CAFCC broken out by complainant province for 2006.

Table 2

	AB	BC	MB	NB	NF	NS	NT	NU	ON	PE	PQ	SK	YK	Total
Prize	83	85	29	34	7	32			342	5	31	40	1	689
Charity	85	57	22	12	1	15			258	4	10	34	1	499
Job	25	34	8	13	1	8			252	2	23	7		373
Directory	26	17	16	4	3	4		2	135	1	99	14	3	324
Office Supplies	33	32	12	9	2	2			116	4	96	9		315
Loan	51	49	16	21	3	14	3		113	6	16	14		306
Merchandise	34	25	12	7	5	5			142		36	5		271
Collection Agency	21	33	11	17	5	12			105		15	5	2	226
Service	27	32	13	6	1	9	1		298		32	7	1	427
Sale of Merchandise	2	20	6	2	1	4			66		11	2		134
Vacation	27	12	20	21	1	12			69	2	1	7		172
Credit Card	10	16	11	3		5			46		15	6	1	113
Investment	17	11	3	1	1	2			45	1	15	3		99
Advertising	7	5	1	2	1		1		40	5	13	2		77
Auction	5	7	2	1		1			38	1	7	2		64

Victim profile

Generally, MMF does not discriminate when choosing targets. Certain demographics may be more susceptible to certain scheme types and solicitation methods. Both RECOL and CAFCC have received complaints from males and females between the ages of 18 and 100. A report released by the Office of Fair Trading in the United Kingdom, "dispels the myth that only the vulnerable, elderly or naïve are taken by scams", and confirms that, "fewer than five per cent of people report scams to authorities". The report further identifies that while both "men and women are likely to be targeted by a scam, incidents do vary by specific scam".[10]

In terms of victimization rates, in-person[11], mail, Internet and print solicitation represent the most effective solicitation methods for Canadian-based MMF operations in duping Canadians. Based on analysis of data to date, it is probable that telemarketing schemes will remain the primary solicitation method reported to CAFCC and it is very likely that mail and Internet-related schemes will continue to increase in 2008.

The data in the next three tables indicate that direct-call fraudsters[12] may be particularly successful against people in their 70s and 80s, and mail fraudsters against people in their 80s and 90s, given the dollar losses for each age group.

10 Office of Fair Trading research into the impact of scams on UK consumers, December 2006. p. 10-11

11 In June 2006, CAFCC received a complaint reporting a 5-million dollar loss to an investment pitch through an in-person solicitation that had been occurring for the past 10 years.

12 Direct-call category refers to telemarketing.

Table 3

	DIRECT CALL			MAIL			PRINT		
Age Group	Attempt	Victim	Dollar Loss Reported	Attempt	Victim	Dollar Loss Reported	Attempt	Victim	Dollar Loss Reorted
10 – 19	14	3	$4,310.00	2	3	$167.80	2	3	$2,594.00
20 – 29	139	24	$48,393.48	28	13	$7,119.95	10	30	$20,863.58
30 – 39	203	25	$67,293.99	34	13	$4,793.89	14	37	$47,004.02
40 – 49	276	34	$155,808.49	76	19	$8,225.29	25	48	$27,425.90
50 – 59	270	32	$127,927.90	67	24	$1,548.10	21	26	$18,426.88
60 – 69	269	36	$110,728.95	69	36	$5,831.52	11	15	$16,913.93
70 – 79	234	44	$239,040.66	85	28	$7,765.61	2	7	$56,535.95
80 – 89	86	33	$214,068.00	54	29	$282,252.33	0	4	$159.85
90 - 99	6	3	$6,550.00	13	4	$302,862.45	0	0	$0.00
BUSINESS	631	151	$257,500.54	85	12	$4,796.09	2	4	$65,795.65
UNKNOWN	449	66	$29,265.55	118	44	$29,465.65	28	16	$255,934.95
TOTALS:	2577	451	$1,260,887.56	631	225	$654,828.68	115	190	$511,654.71

Table 4

	INTERNET / EMAIL			FAX			IN PERSON		
Age Group	Attempt	Victim	Dollar Loss Reported	Attempt	Victim	Dollar Loss Reported	Attempt	Victim	Dollar Loss Reported
10 – 19	8	11	$4,461.00	0	0	$0.00	0	2	$1,491.95
20 – 29	62	102	$97,628.71	0	0	$0.00	6	20	$681,911.88
30 – 39	65	98	$264,734.39	1	0	$0.00	9	34	$443,295.36
40 – 49	60	76	$101,869.08	1	0	$0.00	17	29	$1,352,865.43
50 – 59	40	48	$138,751.44	1	1	$295,000.00	8	24	$761,670.47
60 – 69	23	22	$68,437.41	1	0	$0.00	6	14	$5,167,710.00
70 – 79	5	7	$11,037.90	1	0	$0.00	3	17	$183,518.00
80 – 89	2	1	$4,500.00	0	0	$0.00	2	13	$270,386.25
90 – 99	0	0	$0.00	0	0	$0.00	0	1	$0.00
BUSINESS	32	19	$88,791.12	18	2	$0.00	11	20	$126,509.28
UN-KNOWN	46	32	$38,264.30	0	0	$0.00	27	20	$419,165.50
TOTALS:	343	416	$818,475.35	23	3	$295,000.00	89	194	$9,408,524.12

Table 5

	OTHER / UNKNOWN			REFERRAL			TELEVISION / RADIO / MEDIA		
Age Group	Attempt	Victim	Dollar Loss Reported	Attempt	Victim	Dollar Loss Reported	Attempt	Victim	Dollar Loss Reported
10 – 19	0	1	$939.84	0	2	$1,367.00	0	1	$350.00
20 – 29	8	3	$5,295.00	1	0	$0.00	1	0	$0.00
30 – 39	6	7	$35,121.89	1	4	$61,450.02	0	1	$259.00
40 – 49	9	8	$148,531.77	4	3	$36,465.00	2	0	$0.00
50 – 59	9	7	$1,126.59	1	1	$1,000.00	1	2	$401.80
60 – 69	10	8	$184,906.86	2	1	$851.00	2	0	$0.00
70 – 79	2	5	$11,300.00	0	1	$2,000.00	3	3	$785.20
80 – 89	2	3	$157.75	0	0	$0.00	0	1	$34.97
90 – 99	0	0	$0.00	0	0	$0.00	0	0	$0.00
BUSINESS	31	12	$57,229.09	0	0	$0.00	0	0	$0.00
UNKNOWN	63	19	$112,796.17	1	1	$5,000.00	2	1	$300.00
TOTALS:	140	73	$557,404.96	10	13	$108,133.02	11	9	$2,130.97

Consumers most affected by telemarketing scams are between the ages of 30 and 79, with those between the ages of 30 and 49 reporting the highest victimization rate and complaint rate. Interestingly, the complaint rate for those under 50 and those over 50 is fairly close. 48 percent of complaints received were from consumers under the age of 50 and 52 percent were over the age of 50.

In terms of telemarketing complaints from individuals versus complaints from businesses, 22 percent of the overall telemarketing complaints received at CAFCC were from businesses while 15 percent of telemarketing complaints did not identify an age group.

Schemes involving mail solicitations primarily affected the age range of 60 to 80 with those in their 60s reporting the highest victimization rate. It is likely that schemes marketed through the mail will continue to target seniors based on the increase in mail solicitation from 2004 to 2006.

Internet schemes primarily affected consumers between the ages of 20 and 60 with those in their 20s having the highest victimization rate. A further analysis of data is required to identify which schemes are associated to the Internet.

Schemes involving the Internet give criminals the ability to operate their schemes from any location. The schemes documented are being run at the individual level and at a criminal organization level. For example, Internet auction fraud can be committed by one individual acting alone, while loan schemes that use the Internet to advertise are being operated by organised groups of individuals. West-African Criminal Networks are now using Internet extensively to identify potential victims residing in Canada through various advertising or auction websites, and using emails to communicate with victims.

The CAFCC complaint information documents victims having sent funds ranging from $3.99 to over 1 million dollars. Schemes such as sweepstakes or lottery mail-outs seeking lower dollar amounts ($3.99 – $29.99) are typically used as lead generators to identify victims to target for higher dollar amounts.

Some schemes seek amounts ranging from $199 to $499 but seek to target a larger volume of consumers. Target amounts for scams such as the prize pitch, and 419 pitch, can range depending on the rapport built up between potential victims and fraudsters.

Principal Bases of Canadian MMF Operations

Reported criminal locales are situated primarily in Quebec, Ontario and in British Columbia. Some locales are also reported as situated in Alberta, and some as having connections to the Atlantic Provinces.

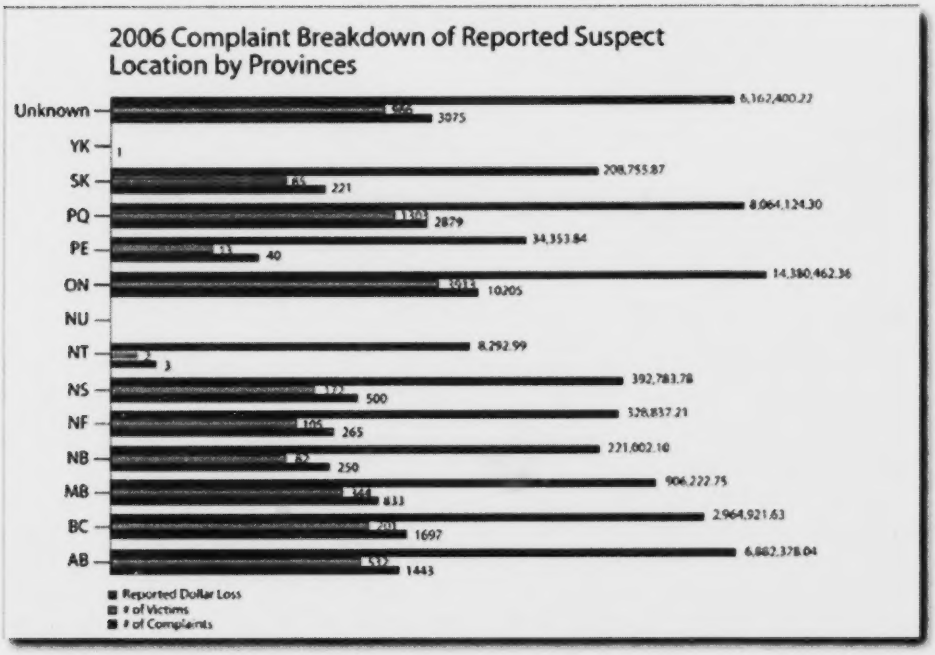
A review of CAFCC briefs indicates that schemes originating in Canada primarily target U.S. citizens. Law enforcement efforts in Canada have greatly assisted to identify Canadian hotbeds for MMF operations such as Toronto, Vancouver and Montreal. While the schemes identified have targeted primarily Canadian and American citizens, complaints have been received from over 25 countries although no significant trends have been identified.[13]

Similarly, these scams are also taking advantage of advances in communication methods, such as Voice over Internet Protocol (VoIP) and prepaid cell phones. While the use of cell phones is not a new phenomenon, MMF operators are increasingly using prepaid cell phones. Their use has allowed for criminal operators to become more mobile, giving them the ability to operate from any location they choose, with any area code and phone number they want. This results in law enforcement challenges in identifying who the criminals are and where they are operating from.

Reported criminal locals in Canada

13 See table, Appendix B

Chart 8

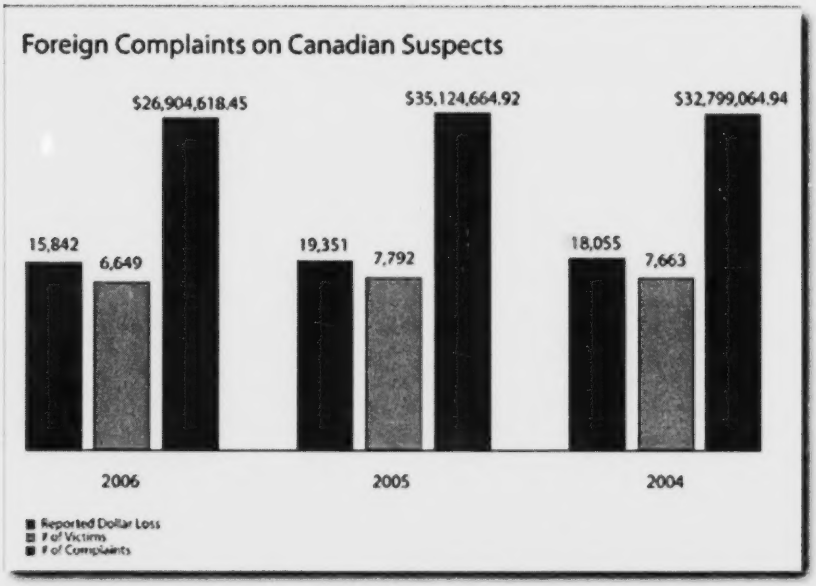


The figures above identify Ontario, Quebec, British Columbia and Alberta as the top ranking MMF criminal locales in Canada, with Ontario accounting for almost half of the reported locations.[14]

In 2006, 73.9 percent of the complaints received at CAFCC on Canadian suspects were received from consumers in other countries. Analysis of incoming calls to the CAFCC toll free line indicates that 37 percent of the calls received are from the United States.

14 Figures were not readily available for 2004 and 2005.

Chart 9



Characteristics of operations within specific locales

Although, Toronto, Montreal and Vancouver remain the three most important locations for MMF operations, there has been an increase in MMF activities in other Canadian cities, mainly Calgary, Winnipeg, Regina and Ottawa. The use of counterfeit cheques by West African Criminal Networks (WACN) to facilitate MMF schemes and the enforcement activities by co-located MMF task forces in the major centres may be factors explaining the dispersion of MMF activities.

The lottery/sweepstake, grants and loans and credit card schemes are operated in all locales. Directory and office supply scams operate primarily from Montreal with some operations in Toronto.

Montreal, Quebec

Top scams investigated by Montreal based Project COLT task force are:

- the *lottery/sweepstake* scams which are mainly targeting Americans and some Canadians;
- the *government grants & loans* scams targeting Americans only;
- the *medical kit scam* targeting some Americans, but mainly Canadians (offenders often pretend to be from Health Canada and Canadian businesses are often targeted;
- the *Medical Programs* scam involving deceptive selling of drugs targeting U.S. victims only – scams involving discounts on purchase of drugs for a fee i.e. $300 - targeting Canadian victims.

Most of the boiler rooms in Montreal are located downtown. Boiler rooms on the Island of Montreal target English speaking victims, mainly U.S. and Canadian victims, depending on the scam.

Prize scams (lottery/sweepstake) are mainly perpetrated through the telephone and involve more significant dollar loss per victim. Individual loss could range from $3,000 to $100,000. These scams are easier to prosecute under the Criminal Code than other types of scams, mainly because the lottery and prizes are completely fictitious. Most scams are clear cut frauds. Most lottery and sweepstake scams (approx. 95%) target seniors.

The grants and loans scams and credit repair scams involve lower amounts of dollar loss, but larger numbers of victims. Most victims targeted have poor credit ratings. In Project CORAL,[15] there was a large number of American victims with average losses of $300 U.S. per victim.

Mass-marketing fraudsters involved in schemes such as grants and loans, credit repair, medical kits, directory, office supplies or anti-telemarketing products, often try to give the appearance of a legitimate form of business.

There have been an increasing number of interdictions involving counterfeit cheques related to schemes run by international criminal organisations.

Toronto, Ontario

Loan, low interest rate credit card, directory, health/medical and prize scams have all been identified and investigated in the Greater Toronto Area.

Loan scams have traditionally solicited U.S. consumers through the use of classified ads in news papers; however, there has been a shift to use the Internet to create websites to advertise fraudulent loan companies, resulting in increased victimization outside the U.S..

Similar to the government grant pitch in Montreal, the low interest rate credit card, and health/medical pitches often aim strictly at U.S. consumers, targeting those with poor credit.

There has been a proliferation of MMF scams involving the use of counterfeit or altered financial instruments. For example, CAFCC has received complaints of job schemes that require the consumer to be a financial agent. Some of these complaints have involved monies going to countries in West Africa and some of them involved money going to Eastern European countries.

Some prize scams that have targeted both U.S. and U.K. residents over the telephone and some are using the mail to target U.S. consumers.

Vancouver, British Columbia

In British Columbia, mainly lottery scams have been investigated. These schemes have solicited both U.S. and U.K. consumers. The lead lists are generated through mail solicitation to participate in a lottery or sweepstakes. Some of the schemes investigated have also been associated to WACN and the use of counterfeit or altered financial instruments. Victims' funds are often received through rogue money transfer businesses and proceeds are laundered through offshore accounts. Some of the activities in British Columbia have been connected to MMF schemes in other provinces.

15 Project Coral – See case summary in Part "G" under "Enforcement" sub-heading

Canadians Targeted by Foreign-Based Operations

As previously noted, MMF schemes have become increasingly global in nature and do not discriminate when choosing potential targets.

Communication methods such as email, Voice over Internet Protocol (VoIP) and the Internet in general are making it easier for criminals to communicate with their intended victims. In addition, the costs of these communication methods are relatively inexpensive compared to the financial gains associated with the scams. In 2006, CAFCC recorded over 12 million dollars in losses reported by Canadians who were targeted by international scams.

In 2006, 62.63 % of Canadian complaints reported to CAFCC involved Canadians solicited by schemes originating in other countries. This confirms that the scope of the threat of MMF is international.

Chart 10

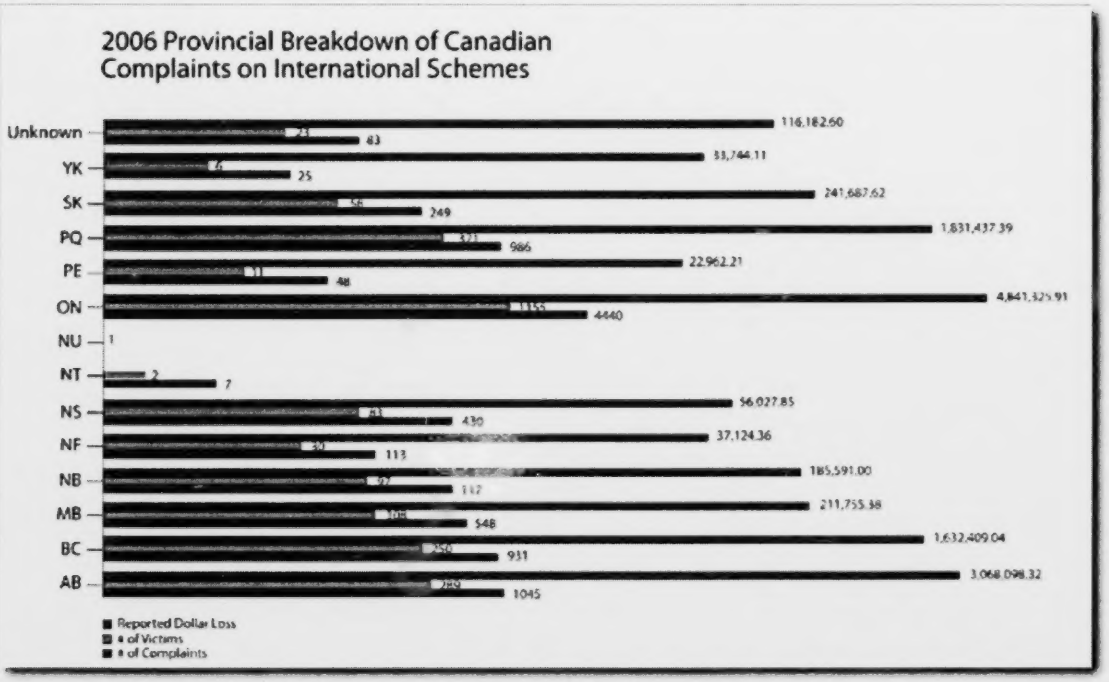
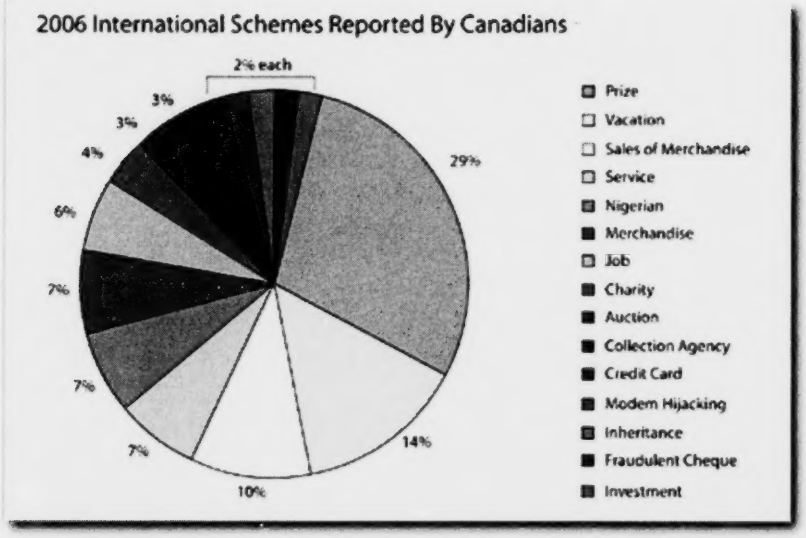


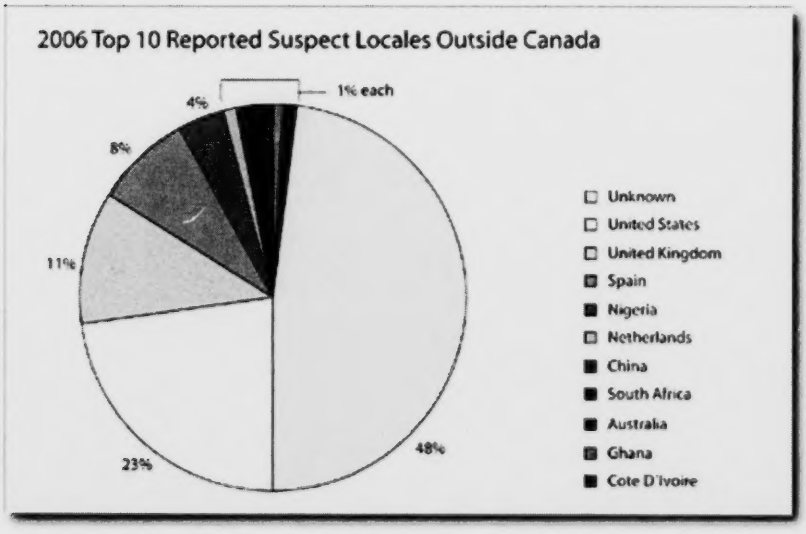
Chart 11



In comparison to schemes originating in Canada and targeting Canadians, international schemes target Canadians at the individual level more so than at the business level. Two of the top five schemes originating in Canada and targeting Canadians identified in 2006 specifically target businesses; they are the directory and office supply scams.

In 2006, CAFCC received 9333 complaints from Canadians reporting suspect locations outside Canada. 5230 complaints identified suspect addresses in 105 different countries.

Chart 12



Again, it must be noted that MMF operation locations are based on suspect addresses reported by consumers, which do not always represent actual suspect locations.

Differences in incidence and prevalence of particular criminal activities

Currently, the most common trend in mass-marketing fraud is the use of counterfeit or altered financial instruments to facilitate mass-marketing fraud schemes. Between March and April 2007, nearly 30 percent of complaints received at CAFCC involved the use of a counterfeit or altered monetary instrument.

The use of counterfeit or altered monetary instruments provides an air of legitimacy to mass-marketing fraud schemes since consumers are not asked to send their own money. Rather, they are asked to cash a counterfeit or altered monetary instrument received from the fraudster and then return the required fees. Commonly, they are used in prize, loan, job and overpayment schemes.

Schemes documented that involve counterfeit cheques are global in nature. Counterfeit cheque schemes are increasingly using Asian bank accounts to facilitate money laundering. Currently the CAFCC has documented bank accounts in South Africa, China, Costa Rica, United Arab Emirates, Ghana, Hong Kong, Japan, Korea, Singapore, Nigeria, United Kingdom, United States, Ireland, Italy and Spain.

Credit Card and Government Grant schemes are facilitated by mail boxes in the United States and almost exclusively target U.S. consumers. They still use traditional boiler rooms, most of which have used or are using VoIP technology.

Some MMF activities can be distinguished by the size, sophistication and type of particular operations. Some MMF operations can be facilitated by one individual acting alone which is less likely to attract attention than an operation with multiple employees doing more volume of business.

In terms of type of scheme being operated, some of the differences are in the methodology of the schemes. For instance, lottery schemes are relatively cheap to operate and aim for high dollar amounts from victims, while government grant and credit card pitches are more costly to operate (office setting) and seek to target larger audiences for lower dollar amounts.

D. Types of Criminal Organizations and Groups

Traditional MMF Boiler Rooms

In Canada, MMF operations exist at both the individual level and organized group level, depending on the scheme being operated. The structure of traditional boiler rooms usually consists of owner(s), managers, and telemarketers and often requires specialized services identified above as facilitators.

Changing profile of MMF operators:

A 2002 research report issued by the Department of Sociology of the University of Tennessee, set out findings from interviews of several convicted fraudulent telemarketers. The description of their profile showed that most came from a middle class background and that they usually had no criminal background.

Since then however, investigations have identified criminal organisation involved in multiple criminal enterprises. One of the suspected reasons for this shift is that MMF operations have the potential of making large money gains at a relatively low risk and low cost. Intelligence derived from investigations indicates that some groups are using the profits to finance their other criminal activities, including the trafficking of drugs and guns.

International Criminal Organisations

In Canada, criminal organisations with international connections have grown or emerged in various locations in the country and have now diversified their fraud activities from the traditional "419" Letter Scams to other types of MMF activities including the lottery, overpayment, job offers and affinity scams. They make extensive use of counterfeit financial instruments, primarily counterfeit cheques, in combination with the fraudulent pitches.

Members of an organisation located in varying countries can be responsible for different aspects of a MMF scheme. For instance some are responsible for sending email solicitation to potential victims, some are responsible for telephone communication with victims and some are responsible for mailing cheques to intended victims.

Ease or Difficulty of Identifying Groups

Generally, MMF schemes are international in scope and make use of technology that is hard to trace such as the use of prepaid cell phones and public email accounts The longer they continue to operate, the more they develop expertise and sophistication in different aspects of advance fee fraud.

Some schemes in Canada are designed to give the appearance of legality and legitimacy by providing products or services, although never ordered, requested or that were not as promised. These schemes are generally operated out in the open as legitimate business fronts and are easier to identify and locate by law enforcement. Examples of these schemes are the government grant pitches and directory pitches. Other schemes are more subversive in their operations and direct in their tactics. They do not provide anything in return for money paid and operate in secrecy to try and avoid detection. These schemes included prize and loan scams.

The use of Internet, VoIP, prepaid cell phones, third party call centres all allow criminal groups to subvert law enforcement in Canada. The use of the Internet and VoIP technology allow scheme operators to operate or give the appearance they are operating from locales other than the ones they are actually operating in. Likewise, MMF operators use prepaid cell phones since fraudulent information can be used on the applications to obtain them.

Third party call centres allow operators to provide victims with contact information other than their own. The third party call centres can also be used by MMF operators to receive notification when an inquiry is made by police or complaints are received.

Financing Sources

As explained previously, some mass-marketing fraud operators may require a minimum amount of resources and infrastructure to operate, while some others may use more complex and expensive infrastructures.

International MMF operations required very little resources and infrastructures to operate the scams. Often, the only thing required is an Internet connection and mail services, which can usually be obtained from any local Internet Café.

Many MMF operators using more sophisticated and costly infrastructures are often individuals who have been operating for several years in the more traditional telemarketing boiler room operations. It is believed that MMF operator finance their new MMF operations with proceeds gained from previous MMF operations.

E. Principal Techniques Used for Fraud

Enablers and Facilitators

Facilitators to MMF activities, whether witting or unwitting, may be used by MMF operations in the various phases of their fraudulent operations, including the initial set up of a scam, the identification of potential victims, reaching and communicating with intended victims, receiving victim funds and laundering of proceeds. Facilitators vary depending on the size and level of sophistication of the group involved. The following facilitators are known to be used by MMF operators in Canada:

Initial Setup and Logistics of Scam

Some schemes require service providers to facilitate office setting, including fax lines, telephone lines (choice of VoIP or traditional hard lines), and Internet connections. Some schemes do not use an office setting but instead operate more loosely through the use of prepaid cell phones, allowing them to be mobile and gather in hotel rooms or residences, or simply operate from their vehicles.

Depending on schemes and sophistication, MMF operations may require several individuals to actually conduct operations, including telemarketers, runners and managers. These individuals are often solicited through job offer adds in news paper, Internet, college and university campuses.

Some MMF operators are using third party call centres for customer services to insulate their activities further. Most of the call centres are located in Canada, but some may also be located outside Canada, such as India. Prize, lottery and sweepstakes schemes are all facilitated through the use of prepaid cell phones.

Identification of Potential Victims

The identification of potential victims is decided upon depending on the intended method of communication with the potential victim and the scam being run. Some schemes such as the West-African 419 Letter scam use email extractors to troll the Internet and pull email addresses of intended targets. Some schemes, including lotteries, sweepstakes and other prize schemes, set up draws at booths in malls and at trade shows. Another method used by fraudsters to identify potential victims is the use mail out lottery, sweepstake or psychic solicitation that require consumer to respond with personal information. Lead lists brokers are also a specialized service usually used to provide telemarketers with list of potential victims. Lead lists are often exchanged or sold between MMF operators. Some scams also simply advertise through media outlets such as newspapers, television, radio, Spam, Internet pop ups or Internet websites to reach potential victims.

Communication with Victims

Communication methods require the use of telephone service providers, Internet service providers, mail/courier providers.

Receiving Money from Victims

Payment methods accepted by MMF operations include money transfer services, bank transfers (including email money transfer), credit card payments, cheques, cash, money orders, bank drafts and PayPal. In 2006, an analysis of overall reported MMF victim complaints[16] to CAFCC identified the following top payment methods used by MMF operations: Western Union (48%), MoneyGram (18%), credit card (5%), cheque (3%), bank wire transfer (2%) and direct withdrawals from victim accounts (2%) (e.g. Automated Clearing House processing).

Laundering Proceeds

MMF operators use the same techniques and enablers as any other type of organized crime activity, such as drug and contraband trafficking, or illegal gambling. For example, they use legitimate company names, offshore bank accounts, nominees, and casinos. They use brokers to convert cash into commodities for reselling.

Solicitation Method and Associated Dollar Loss

MMF schemes are flexible in nature; MMF operators can develop a different pitch for any product, service or event they choose.

Telemarketing (direct call) has ranked the highest amongst solicitation methods used for MMF (including lottery, sweepstakes, credit card, business directories, office supplies, grants and loans pitches) while "in-person" solicitations (deceptive investments scams) consistently yield the highest reported dollar loss. There has been a substantial increase in the use of mail between Canada and other countries, mainly the Untied States, United Kingdom and Nigeria, to facilitate cross-border fraud, particularly for scams used in conjunction with counterfeit financial instruments (cheques/money order) such as lottery/sweepstakes, overpayment and job offers.

16 The analysis did not go into an in-depth break down of top payment methods by specific MMF types.

Overall Canadian targeting Canadian Mass Marketing Fraud dollar loss for last 3 years by solicitation method is shown in the table below:

Table 6

	DIRECT CALL			MAIL			PRINT		
Year	Attempt	Victim	Dollar Loss Reported	Attempt	Victim	Dollar Loss Reported	Attempt	Victim	Dollar Loss Reported
2006	2677	468	$1,268,009.78	655	229	$655,362.52	118	192	$513,645.16
2005	3158	586	$1,612,003.05	700	212	$145,249.43	115	164	$393,414.99
2004	3319	499	$2,781,080.59	428	216	$34,787.27	189	189	$431,978.18
TOTAL	9154	1553	$5,661,093.42	1783	657	$835,399.22	422	545	$1,339,038.33
	INTERNET / EMAIL			FAX			IN PERSON		
Year	Attempt	Victim	Dollar Loss Reported	Attempt	Victim	Dollar Loss Reported	Attempt	Victim	Dollar Loss Reported
2006	350	421	$858,066.51	23	3	$295,000.00	92	199	$9,419,999.12
2005	282	492	$1,054,323.78	30	5	$133,066.67	137	220	$3,139,333.70
2004	283	321	$930,964.37	40	13	$4,417.80	148	147	$1,189,849.89
TOTAL	915	1234	$2,843,354.66	93	21	$432,484.47	377	566	$13,749,182.71
	OTHER / UNKNOWN			REFERRAL			TELEVISION / RADIO / MEDIA		
Year	Attempt	Victim	Dollar Loss Reported	Attempt	Victim	Dollar Loss Reported	Attempt	Victim	Dollar Loss Reported
2006	148	79	$561,754.96	10	13	$108,133.02	11	9	$2,130.97
2005	183	163	$2,570,983.62	9	16	$1,969,292.08	9	11	$748.84
2004	167	140	$1,791,416.09	7	10	$61,218.93	3	13	$8,702.72
TOTAL	498	382	$4,924,154.67	26	39	$2,138,644.03	23	33	$11,582.53

Overall in the last 3 years, Telemarketing (direct call) has ranked the highest amongst solicitation methods in terms of the number of reported occurrences and is followed in order by mail, Internet, print, and in-person. In terms of dollar loss, in-person solicitations consistently yield the highest reported dollar loss. This can be attributed to what the American Association of Retired Person call the perpetrators involved in in-person schemes — "trusts". The AARP documents that "trusts" have a huge advantage since the victims know them before the crime begins, "they are their family, friends, neighbour, a new sweetheart, their caregiver..."[17]

In terms of victimization rates, in-person (60%), mail (60%), Internet (57%), and, print (56%) solicitation represent the most effective solicitation methods in duping Canadians. Based on analysis of data to date, it is probable that telemarketing schemes will remain the primary solicitation method reported to CAFCC and it is very likely that mail and Internet-related schemes will continue to increase in 2007.

17 http://www.aarp.org/research/international/speeches/june15_06_shutme.html

F. Receipt and Laundering of Mass-Marketing Fraud Proceeds

Principal Means and Conduits to Receive Funds from Victims

While initially funds were forwarded to the fraudster by way of a cheque or cash through the mail stream, new methods are being used to receive funds from victims. Money transfer businesses appear to be increasingly used for this purpose.

With more than 250,000 and 100,000 worldwide locations respectively, cash payment outlet services provide a global network of agents located in businesses such as convenience and grocery stores, travel agencies, cheque cashing businesses and currency exchanges. The process of collecting fraudulent funds at those counters is either done through the use of fraudulent identification documents or with the complicity of the money transfer agent. All that is needed to collect the money is the transfer control number and funds can be picked up at almost any location. Fraudulent activities being committed using the Internet as the primary means of communication and transaction, payments are usually received via Internet Payment Systems (IPS).

The following graphics show the reported methods of payment made to specific countries:

Chart 13

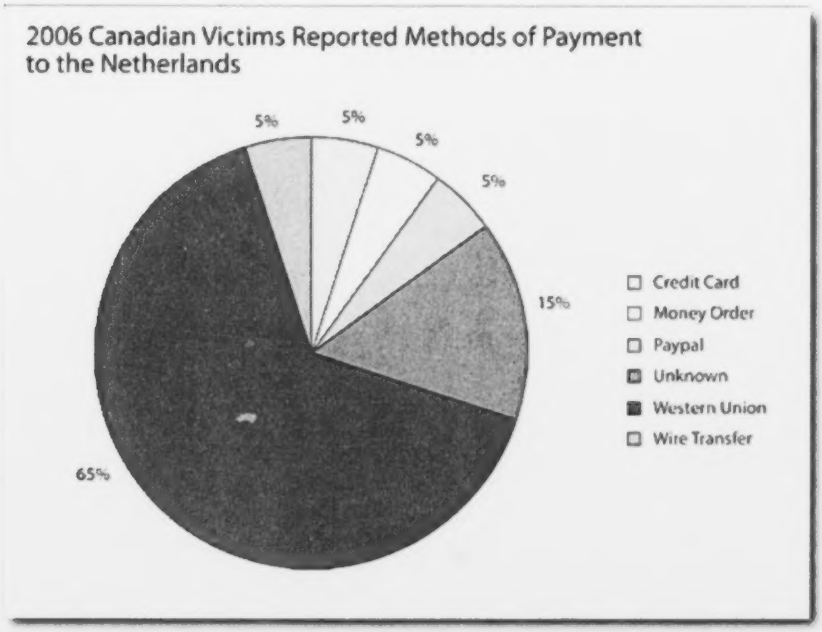


Chart 14

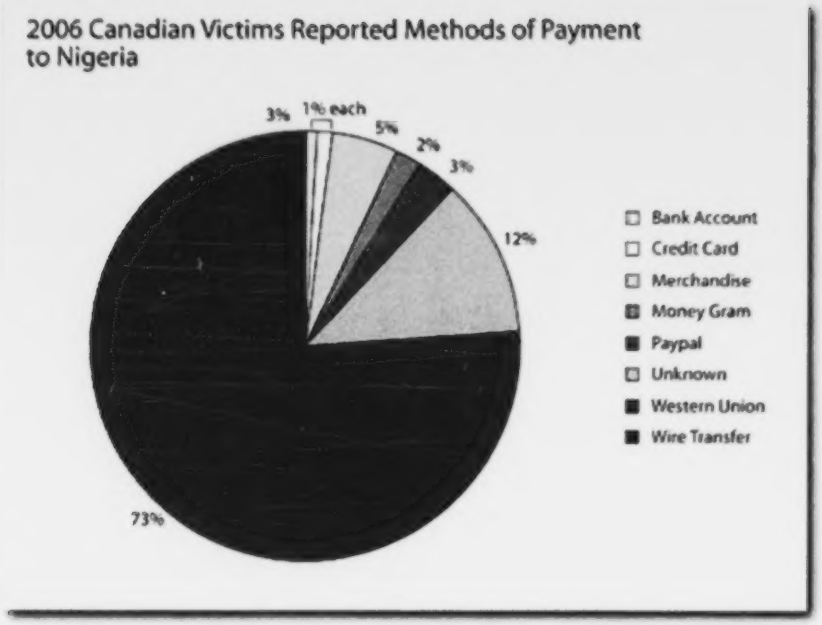


Chart 15

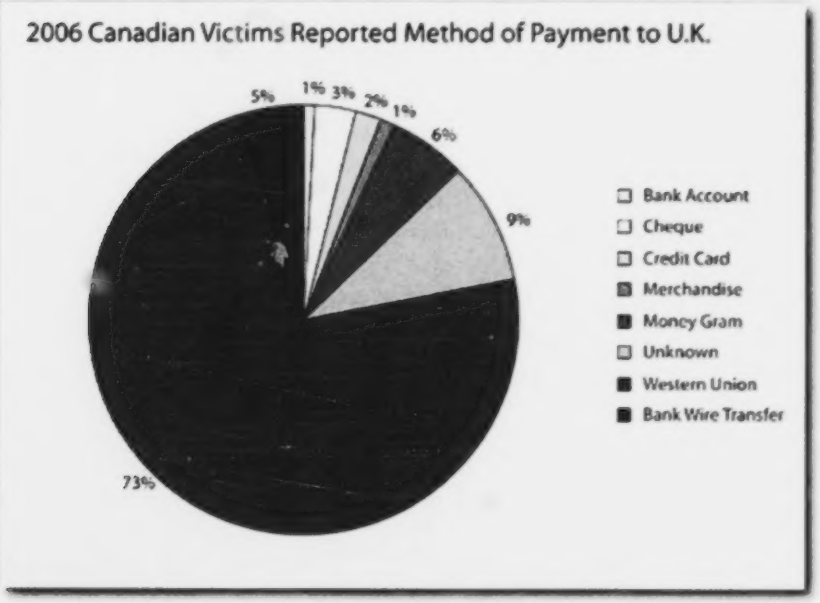
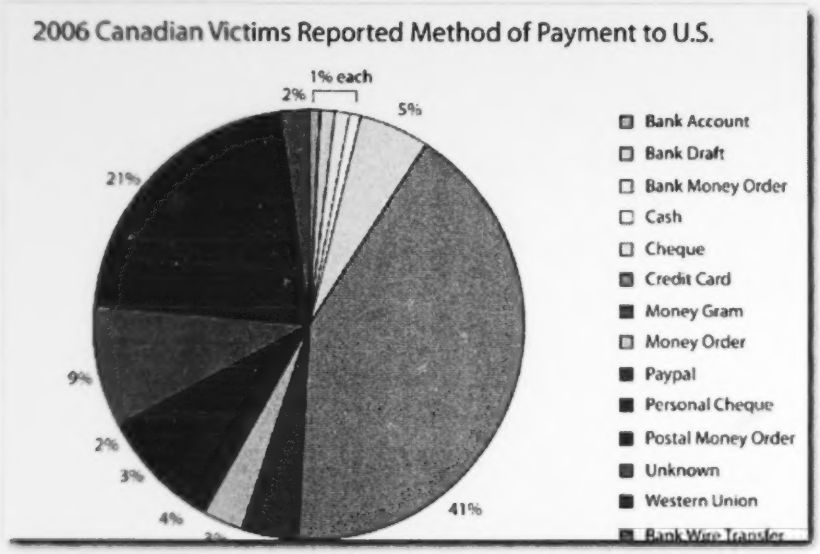


Chart 16



Principal Means and Conduits to Launder Funds after Receipt from Victims

On the money laundering front, organized crime will exploit every new opportunity to launder their proceeds of crime. Some of the current methods that have been used for some time are: "smurfing"[18], electronic funds transfer, the use of money service businesses, casinos, credit cards and co-mingling of funds using legitimate businesses. Furthermore, a few emerging trends that have been investigated lately and that are particularly of interest to the laundering of proceeds obtained from mass-marketing frauds are: money laundering through Internet Payment Systems (IPS), prepaid credit cards and digital currencies.

As proceeds from mass-marketing fraud are being received by way of a cheque or cash — and also through Internet Payment Systems (IPS) it needs to be laundered in order to distance it from the original crime. While a cheque needs to be deposited into a bank account for further electronic funds transfers into other bank accounts in order to blur the paper tail, cash can be introduced into the financial systems via other means. Prepaid credit cards and digital currencies are increasingly used in the laundering process as it provides several features of interest for money launderers such as anonymity, cash-based, global reach and worldwide transfer features.

18 Money laundering technique consisting of making deposits just below the reporting threshold in various bank accounts housed in multiple banks.

Money Laundering through Internet Payment Systems (IPS)

The particularity of IPS is that money can be sent around the world without going through the normal path of the worlds' banking system. In essence two users registered with an IPS can send money between their accounts in the click of a button and at a very low cost. The usual method to fund the account is through an electronic funds transfer (EFT) from a bank account. You can also attach a credit card to the account to settle payments using the IPS. Three options are available to withdraw funds from the IPS: EFT to a bank account, merchandise purchase at IPS shops and withdrawal at an automated teller machine (ATM) using debit / credit card.

There is certainly a presence of risk concerning money laundering and IPS. The IPS can be used as a tool in the laundering process, particularly in the layering stage where funds can be sent to various countries worldwide. It could also be used in the placement stage as a vehicle to "receive" proceeds of crime within the account. This will prevent the individual involved in criminal activity from being stuck with a large amount of cash that will then have to make its way to the bank. This feature is of particular interest for mass-marketing fraud committed over the Internet.[19]

Complex schemes could potentially be developed where several money transfers would occur in various countries where the individual has bank accounts. Money would be transferred from the IPS account to the bank accounts. Other EFTs could then be sent to other bank accounts or bank drafts could be issued from these accounts for further movement of proceeds of crime.

Some IPS providers, are monitoring "suspicious" activities so that large money transfers between accounts for no specific or business reasons will probably be "questioned" or prevented by the IPS if no satisfactory explanations are given by the account holder. However, the use of "front stores" for sending false invoices to customers in other countries could potentially bypass the monitoring of "suspicious" activities and large amounts of money could be transferred around the world.

Money Laundering through Digital Currencies

E-currency refers to a digital form of currency issued by private companies. The e-currency sector is composed of e-currency "issuers" and e-currency "exchange agents" who work closely together in order to enable clients to conduct their e-currency based financial transactions. The issuer of the e-currency guarantees its value usually in the form of gold and other precious metal holdings and provides financial services (e.g. cheque accounts, electronic funds transfers, etc.) that are similar to the ones offered by regular financial institutions. In order to buy these e-currencies, individuals will use different types of payment such as: electronic funds transfers, money orders, cash, gold, personal cheques and other e-currencies.

The main problem of e-currency, from a money laundering perspective, is that once the funds are within an e-currency account, they become untraceable due to the fact that e-currency networks are operated by private corporations and outside the financial system. Individuals are therefore able to send funds around the world virtually without any "paper trail" or financial records since all transactions are processed on a private computer server owned by the e-currency "issuers" or "exchange agent".

Also, some of these e-currencies "issuers" or "exchange agents" even offer debit cards that are linked to their corresponding e-currency account. This feature allows the holder of the debit card to obtain local currencies, services and goods around the world at any ATM or Point of Sale outlet.

Money Laundering through Prepaid Credit Cards

Prepaid credit cards have only appeared recently within the Canadian market. These cards can have a reloadable or non-reloadable feature. Due to the fact that the prepaid credit card market is fairly new in Canada, it is difficult to estimate its size. However, it would not be unreasonable to estimate the Canadian market at several billion dollars.

There are several money laundering concerns associated with these cards. The first concern relates to the identification process. It appears to be limited as only basic identification is required and some ID numbers requested for identification purposes (e.g. foreign passport number) are difficult to verify. In some instances not even the date of birth is requested.

Furthermore these cards are considered somewhat of a cash-based product. Even though several reloadable options are offered to clients, the cash feature may be problematic especially if card limit are significantly high.

Another concern relates to the cross-border movement of currency. Cash cards are not defined as monetary instruments under Part 2 of the Proceeds of Crime (Money

19 Although we have no particular example of this, the key point here is that the feature is of interest, it may be exploited by fraudster.

Laundering) and Terrorist Financing Act, R.S.C. 2000, c.17. Furthermore, there are no card readers at the border crossings in order to determine the amount of money loaded onto these cards. The card-to-card transfer also can be problematic for cross-border movement of currency. For example someone can buy two cards, send one to the United States, via mail, and transfer money from his card in Canada to the one located in the United States. Because both cards were purchased in Canada, the transfer between cards, regardless of the amount, is not reportable because it is defined as a domestic transfer. All of the prepaid credit cards offer worldwide ATM access and the cash obtained is in local currency.

The final concern is that a cash card can be loaded using e-currency. As stated before, the main problem of e-currency, from a money laundering perspective, is that once the funds are within an e-currency account, they become untraceable due to the fact that e-currency networks are operated by private corporations and outside the formal financial system. E-currency transactions are processed through computer servers owned by private companies.

Estimates of Volume of Laundering of Mass-Marketing Fraud Proceeds

Several cases investigated in Canada show that mass-marketing fraud operations can generate substantial amounts of revenues in a relatively short period of time.

For example, in Montreal, Project CORAL[20] unveiled a criminal operation which generated over $30 million U.S. in 18 months.

In a case investigated by Project EMPTOR, a fraudulent scheme operated by a B.C. couple which involved selling credit card protection to customers in Los Angeles and across the United States, took in more than $10 million from thousands of victims.

In Canada, there are no clear estimates to show the extent and volume of money laundering from mass-marketing fraud proceeds. In many cases it is more difficult to trace and seize proceeds because the money is split amongst the group in cash.

Identification of Money Couriers and Comptrollers

Information derived from investigations and complaints received from the public clearly indicate that mass-marketing fraud operators make extensive use of money transfer/exchange businesses for transfers involving transactions of less than $10,000. Cashier's cheques and bank-to-bank wire transfers are the most common methods for transactions involving amounts of $10,000 and above.

Cashiers cheques are sent to addresses using mail drops. Some individuals are being paid for using their mailing address. There is a burden to prove the individuals had knowledge of the fraud. However, currently most transactions use wire transfers; bigger amounts are normally bank-to-bank transfers.

Cash is usually sent through courier services or regular mail. The Intercept Program[21] is a good disruption practice. The amount of money sent by victims can range from $3,000 and go as high as $100,000.

Investigations have identified that criminals use of Casino to withdraw large sums of money where the limit can be $25,000 for point of sale withdrawals. This method is used by criminals to withdraw cash out of their bank accounts which are used to receive funds from victims through bank-to-bank transactions. There is normally a maximum limit per transaction/per day (example $500.00) for withdrawals, when the transaction is done through a regular ATM machine or merchant point of sale. However, the casino allows withdrawals of up to $25,000.

Some money laundering operations from mass-marketing fraud proceeds are facilitated through the use of numbered companies and offshore bank transactions. Complaint information received at CAFCC has idenitified bank accounts in Japan, United Kingdom, Netherlands, Germany, United States, Isreal, Nigeria and several other countries.

20 Project Coral – See case summary in Part "G" under "Enforcement" sub-heading.

21 Intercept Program – See description in Part "G" under "Disruption" sub-heading.

G. Current "Best Practices" for Reducing Incidence and Prevalence of Mass-Marketing Fraud

The National Mass-Marketing Fraud Working Group (NMMFWG), chaired by the Competition Bureau, Ontario Provincial Police and the RCMP, developed a national strategy in order to *dismantle, disrupt and neutralize Canadian-based MMF operators.* To achieve this goal the working group identified three core objectives: 1) Increase the business risk and cost for MMF operators; 2) Strengthen law enforcement effectiveness 3) Decrease victim susceptibility.

To accomplish the core objectives, partners and stakeholders must initiate innovative measures which, over time, could become "best practices".

Intelligence

The Canadian Anti-Fraud Call Centre (previously know as "PhoneBusters") and Reporting Economic Crime On-Line (RECOL) are the main central points for collecting complaint information regarding MMF which is then analyzed by the analytical unit at the CAFCC.

Initiated by the OPP in 1993, Project PhoneBusters is recognized as the earliest attempt at centralizing telemarketing fraud complaints and complaint taking. The original mandate of PhoneBusters included centralized complaint taking and investigations of occurrences of telemarketing fraud in Ontario. It became clear at an early stage of the project that telemarketing fraud operators targeting Ontario residents were not in Ontario but in Quebec. It also became clear that Ontario residents were not the only consumers being victimized.[22]

Canadian criminals engaged in MMF schemes victimize Canadians, Americans and citizens of other countries. Criminals are taking advantage of globalization and new technologies to perpetrate their fraudulent activities. Criminals use jurisdictional borders to their advantage to avoid detection and resort to increasingly elaborate and complex methods to commit their crimes, rendering law enforcement's investigations more daunting and greatly reducing the offenders' risk of facing prosecution.

By 1997, it was widely recognized that MMF was not just a Canadian phenomenon. The data collected exclusively at PhoneBusters was a valuable tool in evaluating the effects of fraud on Canadians, greatly enhancing the ability of government and law enforcement officials to prevent, reduce and respond to the consumer threat of MMF.[23]

Today, PhoneBusters is known as The Canadian Anti-Fraud Call Centre (CAFCC) and plays a key role in education and prevention of mass-marketing fraud schemes while promoting the principles of intelligence-led policing through the collection, analysis and dissemination of complaint and victim information to law enforcement agencies of jurisdiction.

As well, in 2003 the RCMP launched a web-based fraud reporting system called Reporting Economic Crime OnLine (RECOL). The secure site was designed to accept fraud complaints worldwide provided that there was some Canadian content such as a victim, or a suspect located in Canada. RECOL is also designed to automatically

22 http://www.phonebusters.com/english/aboutus.html

23 http://www.phonebusters.com/english/aboutus.html

distribute the complaints meeting a certain priority level to police of jurisdiction. The ultimate goal of RECOL is real-time automated information sharing between law enforcement and regulatory agencies with a vested interest in receiving consumer fraud complaints.

Centralization of fraud complaints is a key element to enable better information sharing and the development of intelligence. The CAFCC and RECOL databases are being merged, which will allow accepting any type of fraud complaint with a Canadian content, either through the telephone, mail, fax or the internet. Regardless of location, any person or organization would be able to lodge a complaint or share information with the appropriate law enforcement body.

Enforcement

Partnerships and Task forces

In Canada, the six MMF partnerships, which include three co-located task forces, are the main enforcement bodies to investigate, disrupt and dismantle MMF Operations.

Since MMF operations are centered in major urban centers, namely, Toronto, Montreal and Vancouver, partnerships and task forces were created in these areas. Even though this is an ad hoc response to MMF, each partnership and task force has developed specific aims that are based on their respective membership. These joint force operations need to respect each partner's mandate to maintain a sufficient level of commitment. The success of these partnerships and task forces has laid the foundation for a continuing and growing enforcement of MMF.

Project COLT

Often considered the first task force in Canada, Project COLT was officially established in 1998 and it is led by the RCMP. COLT is a joint force effort to combat Canada-based criminal fraudulent telemarketing schemes. Partners include DHS ICE, the Sûreté du Québec (Quebec Provincial Police), the Montreal City Police Service, the Canada Border Services Agency (CBSA), the FBI, the Competition Bureau, the FTC and the U.S. Postal Inspection Service.

The focus of Project COLT is to identify, investigate and disrupt organizations perpetrating these schemes and seize the proceeds of their operations, as well as return money to victims of telemarketing fraud. This is accomplished through three strategies: investigations, interceptions and prevention.

Highlight of Project COLT Enforcement Activities:

Between 2004 and 2006, Project COLT opened more than 500 MMF related files and received over 2000 complaints that involved more than $75 million dollars in reported losses relating to telemarketing fraud.

As an intelligence-led task force, COLT undertakes major investigations that seek to identify and target higher levels of the criminal organizations involved in MMF. Through this project approach COLT has been very successful in identifying that criminal organizations involved in MMF activities are often involved in multiple criminal enterprises.

The following summaries provide an overview of the specific investigations undertaken by COLT and the nature of MMF operations in Quebec:

Project CORAL

Project CORAL was a 2004 investigation of an MMF operation based in Quebec that targeted U.S. residents. This investigation was initiated as a result of a request from the Department of Homeland Security (DHS) Immigration and Customs Enforcement (ICE). The scheme initially involved the sale of credit repair kits but switched to government grants and loans, with each sale being approximately $299.00 US. In a six month period approximately 2.2 million calls were made. The operation ran a number of boiler rooms, some of which had Voice over Internet Protocol (VoIP) technology and required technical assistance to dismantle the computer and telephone systems. A corrupt bank employee in the U.S facilitated the transfer of funds from victims. Over a seventeen-month period, the group is estimated to have grossed $30 million dollars.

Project CASINO

Project CASINO was initiated in 2003 to investigate an international telemarketing fraud operation, which involved an advance fee lottery/prize scheme. The victims were from the United States and the United Kingdom and some lost up to $100,000 US. Seven subjects were arrested in Montreal and charged in the United States.

Toronto Strategic Partnership

The Toronto Strategic Partnership was created in 2000 as part of a broad initiative by the U.S. and Canadian governments to enhance cooperation between the two countries in fighting fraud. The members include the FTC, the USPIS, the Toronto Police Service Fraud Squad, the Ontario Ministry of Government Services, the OPP Anti-Rackets, Competition Bureau Canada, the RCMP and the Office of Fair Trading, United Kingdom.

Highlights of Toronto Strategic Partnership Enforcement Activities:

Although, information on the exact number of files opened from 2004 to 2006 was not available, a Toronto Partnership report, *The First Six Years: Accomplishments of The Toronto Strategic Partnership*, presents a review of 37 significant cases. The report points out, that while they do not have accurate data, they believe "the numbers they provide are conservative" and are "confident that the total losses exceed the figures they have provided."[24]

Three files were identified in the report for the period of 2004 to 2006. The files identified involved schemes that are estimated to have defrauded over 500,000 victims and netted over $200 million in net sales. The Toronto Partnership focuses on quickly identifying and dismantling MMF operations. Relying on tactical and operational intelligence to identify MMF operations, and CAFCC and Consumer Sentinel for complaint and victim information, the partnership has been successful in eliminating the credit card pitch from the Greater Toronto Area (GTA). The Partnership coordinates any investigations with all partners, so as to effect action not only under the Criminal Code, but also the Competition Act, FTC civil actions and possible extradition to the U.S.

The following summaries of cases demonstrate the complexity and range of schemes operating out of the GTA:

Project CENTURION

Project CENTURION was a 2005 investigation of a telemarketing scheme that solicited U.S. consumers with false credit card offers for an upfront fee of $249. Consumers who agreed had their bank accounts debited by a third party processor but did not receive a credit card and instead received applications for stored value cards.

This investigation involved the largest room ever taken down by the partnership with one room housing over 150 employees. It is estimated that this group was responsible for defrauding over 120,000 victims and generating $35 million dollars. The boiler rooms all had VoIP telephone systems, and required technical assistance to dismantle the computer and telephone equipment found in the rooms.

Project SPIN MARKETING

Project SPIN MARKETING was a 2005 investigation of a lottery scam targeting U.S. citizens. The scheme involved two phases. During the first phase, the consumers were told they had won a lottery but had to pay a release fee by credit card, cheque or money order. During the second phase, the scam targeted seniors to pool their money to purchase lottery tickets. A few tickets were purchased and photocopied to lead victims into believing they had entered a large lottery pool.

Other notable cases include:

Trader's International, was a false invoicing scam for office supplies and advertising that targeted businesses in more than 25 different countries.

Project IMPACT was a Toronto Police Guns and Gangs project that involved telemarketing loan schemes targeting U.S. consumers.

Project EMPTOR

Project EMPTOR was established in 1998 and is an RCMP-led multi-agency task force which investigates illegal telemarketing activity. Its partners include the Business Practices and Consumer Protection Authority (BPCPA) of BC, Competition Bureau Canada, FTC, USPIS, and FBI.

The focus of Project EMPTOR is to identify and disrupt, high level telemarketing operations working out of British Columbia, through asset seizures and criminal charges. Project EMPTOR utilizes a three pronged response involving investigations, interceptions and education.

Unique to EMPTOR is the use of Provincial laws (BPCP Act) in tackling some of the scheme operators. In addition, EMPTOR uses MLATs to facilitate arrests and the extradition of MMF operators. The following case summary is an example of an MMF scheme in British Columbia:

EUROBOND

This investigation was initiated in 2004 and targeted a scheme that involved calling people in the U.S. and offering bonds from other countries. Part of the pitch also involved telling potential buyers that if they purchased a bond they would be entered for a chance to win a prize. Thousands of complaints were identified with over $3 million dollars U.S. in losses.

Alberta Partnership Against Cross-Border Fraud

Initiated in 2003, the Alberta Partnership Against Cross-Border Fraud is a bi-national partnership of law enforcement agencies working together to identify, prevent, investigate, combat and control deceptive marketing practices and fraudulent criminal activities originating from Alberta or

24 The First Six Years: Accomplishments of The Toronto Strategic Partnership, January 2007.

impacting on Alberta. The partnership agencies include: Services Alberta, Calgary Police Service, Competition Bureau, Edmonton Police Service, RCMP, FTC and USPIS.

Between 2005 and 2006, the Alberta Partnership identified and investigated prize, credit card, pyramid, directory, job and Ebay schemes. The following case summary identifies some of the characteristics of MMF in Alberta:

Centurion Financial

With the assistance of the CAFCC, the Alberta Partnership identified a boiler room soliciting an advance fee credit card pitch targeting U.S. consumers. The boiler room activity was directly linked to the Centurion investigation in Toronto. It also used VoIP technology and a third party processor to debit consumer accounts.

Vancouver Strategic Alliance

The Vancouver Strategic Alliance was formed in 2004 as a joint venture between The Competition Bureau, Vancouver Police, the British Columbia Business Practices and Consumer Protection Authority (BPCPA), USPIS and the U.S. FTC. The Office of Fair Trading in the U.K. is in the process of joining the partnership. The purpose of the partnership is to identify and investigate, prosecute and disrupt fraudulent telemarketing activity which originates in the Vancouver area.

Atlantic Partnership Combating Cross-Border Fraud

Created in 2005, the goal of this partnership is to identify, investigate and prosecute, and thereby reduce deceptive marketing practices and fraudulent criminal activities originating from the Atlantic region and targeting American consumers or from the U.S. and targeting Atlantic Canada. Partners include the RCMP, Canada Post Corporation, Charlottetown Police Department, Competition Bureau Canada, Halifax Regional Police, Office of the Attorney, General of N.B., Royal Newfoundland Constabulary, Saint John Police Force, Service Nova Scotia and Municipal Relations, FTC, and USPIS.

In 2006, the partnership began two MMF files, one involving an Online Directory and one involving a prize scheme involving counterfeit cheques.

Summation of Investigative Data

Cases reviewed identify that in the last three years, prize, loan, government grant, credit card, directory, health and investment pitches have been targeted in Canada. Most investigations handled by the partnerships and task forces are cross-border frauds between Canada and the United States and some have involved victims in the United States and Canada. No investigations involved Canadian victims being targeted solely by Canadian-based MMF operations or by scams originating in other countries.

Disruption

Interception Program:

The Intercept Program is an efficient strategy to disrupt Cross-Border MMF operations. This program involves the interception of cash and negotiable instruments as they enter Canada being sent by victims in the U.S. and elsewhere and destined to fraudsters. The RCMP continues to encourage participation of key partners in the Intercept Program (Canada Border Services Agency, postal services, and courier services). Millions of dollars are intercepted annually and returned to victims.

COLT and EMPTOR are RCMP Commercial Crime Section led multi-agency task forces that combat mass-marketing fraud operations out of Montreal and Vancouver respectively. Since the inception of the MMF task forces, the Canadian Border Services Agency (CBSA) has been a key contributor in the concerted efforts to curb Mass Marketing Fraud. CBSA has been instrumental in intercepting large sums of money originating outside Canada, mainly from unsuspecting elderly victims from the US or the UK, en route to Canadian mass-marketing fraudsters.

In 2004, through the Intercept Program, EMPTOR intercepted and returned approximately $865,000 in cash and negotiable instruments. They also intercepted $14.2 million in counterfeit cheques that were outbound, en route to victims in the USA. At least some portion of these would have been acted upon by victims. In 2005, EMPTOR intercepted approximately $1 million in cash and negotiables and $118 million in counterfeit cheques. Since 1998, with the assistance of CBSA, COLT intercepted $5,884,305, which otherwise would have made its way into the hands of criminals. The support of CBSA has been instrumental in preventing further victimization and allowing the return of money to the victims. The Intercept Program is highly valued by US partner agencies.

In all cases of recovery/intercept, total cooperation was required between the private sector (wiring service), regulatory and police agencies on both sides of the Canada-U.S. border.

Knock and Talk Program

The Knock and Talk Program is one of the disruption activities undertaken within the parameters of the COLT Interception /Prevention Team in Montreal. At least once a month, the entire COLT team goes out and actively does "Knock and Talks" at Montreal area boiler rooms. Target boiler rooms are selected from information received from the Canadian Anti-Fraud Call Centre (Phonebusters) or complaints received directly from the public.

The objective is to get boiler rooms to shut down or at least disrupt their operations, following the visit of law enforcement.

In order to have the most impact "Knock and Talk" activities are co-coordinated with COLT partners: RCMP, SQ, SPVM, Competition Bureau, FBI, Dept. of Homeland Security — Immigration and Customs Enforcement, U.S. Federal Trade Commission, and U.S. Postal Inspection Service. Canada Revenue Agency is also included in these activities.

Prevention and education

The Canadian Fraud Prevention Forum.

March is Fraud Prevention Month in Canada and around the world. During the month, Fraud Prevention Forum members raise awareness of the dangers of fraud, while educating the public on how to: *"Recognize it. Report it. Stop it."* The Forum, which is chaired by the Competition Bureau, is a concerned group of private sector firms, consumer and volunteer groups, and government and law enforcement agencies committed to fighting fraud aimed at consumers and businesses. The Forum has been growing almost exponentially year after year with various organizations from law enforcement, government and the private sector.

SeniorBusters

In 1999, PhoneBusters initiated SeniorBusters, a volunteer program presently consisting of approximately 60 volunteer members over the age of 50. The concept behind SeniorBusters is based on seniors talking to seniors, as this particular demographic has historically been more vulnerable to scams. These volunteer members come from diverse backgrounds and bring many different skills to the SeniorBusters program, in its attempt to reduce the level of fraudulent telemarketing against seniors. SeniorBusters will contact family members, local police agencies, elder abuse committees, and provide the seniors with the necessary tools to effectively prevent victimization.

Conclusion

Mass Marketing Fraud remains a problem in Canada and is causing severe harm to Canadians and foreigners alike. The MMF activities in Canada range from the simple to complex schemes and are often international in scope. They affect Canadians financially and can reduce consumer confidence.

Mass-marketing fraud is perceived by criminals as a high-profit low risk criminal activity. For criminals engaged in MMF activities, these perceptions have contributed to a risk-reward ratio that is totally out of balance; there is the view that the potential rewards for continuing to perpetrate scams and frauds in Canada greatly outweighs the remote risks of detection and prosecution attached to this activity. MMF therefore remains an extremely attractive criminal venture.

While mass-marketing fraud operations continue in Canada, similar operations in other countries are on the rise. The following factors can be associated to the expansion and globalization of mass-marketing fraud operations:

- Although telephone and mail remain widely used by mass-marketing fraud operators, the Internet has enabled criminals to expand their victim-base market and reach out to potential victims almost anywhere in the world at very low cost.
- Computer software, hardware and printers are now available at affordable costs and widely used by fraudsters to produce counterfeit financial instruments.
- New telecommunication technologies allow criminals to operate covertly and in almost any geographic location.
- Electronic payments, bank wire transfers, cash payment outlets are facilitating the reception by criminals of money from victims and the laundering of proceeds of crime across jurisdictions.

International fraud schemes continue to be a problem. These activities have evolved to the extent that a large part of the scams now involve counterfeit cheques. Generally, these schemes are run by criminal organisations that are international in scope and have developed strategies that inherently subvert criminal investigations through the use of prepaid cell phones and public email accounts. The structure and continuity of these networks give them stability and allow for them to develop expertise and sophistication in different aspects of advance fee fraud.

A new trend is the mass distribution of counterfeit cheques using the cover of legitimate businesses. Potential victims are lured into cashing a cheque and returning a portion of the amount to the criminals.

MMF operations identified in Canada have been primarily situated in Ontario, Quebec, British Columbia and Alberta. Likewise, there are more victims in areas with larger populations. Both CAFCC and RECOL complaint data support that Ontario is the largest hub in Canada for both MMF operations and victimization.

MMF schemes operating in Canada are not limited to targeting Canadians and some have established global networks to facilitate receiving victim funds, such as the WACN use of Asian bank accounts.

Cases reviewed identify that in the last three years, prize, loan, government grant, credit card, directory, health and investment pitches have been targeted in Canada.

Most investigations handled by the partnerships and taskforces are cross-border frauds between Canada and the United States and some have involved victims in the United States and Canada. No investigations involved Canadian victims being targeted solely by Canadian-based MMF operations or by scams originating in other countries.

In the last three years no information has been available to detail, or that could be used to detail, the number of MMF operations in Canada.

Investigative data reviewed did not always identify money laundering patterns or the final destination of MMF proceeds.

Information collected from investigations in the last three years could not determine whether there are MMF operations in Canada only affecting Canadians. The scope of MMF is international and all existing partnerships and taskforces include a U.S. presence.

Investigative data gathered only identified information on the scheme types, associated dollar losses, and associated victim numbers. Without surveying law enforcement and regulatory agencies responding to MMF incidents, intelligence gaps exist in the collection of investigative data.

Telemarketing (direct call) is the highest reported solicitation method used for MMF schemes, and "in-person" solicitations consistently yield the highest reported dollar loss. There has been a substantial increase in the use of mail to facilitate cross-border fraud between Canada and U.S.

The comparative analysis of the top twelve scams provides a basis for identifying MMF activities and trends posing the greatest threat to Canada. The first five schemes in order are: prize (including lottery and sweepstakes) pitches, the work at home/ job opportunities, foreign money offers (419 scams), loan pitches and overpayment (sale of merchandise) scams. All of these have been associated to the use of counterfeit or altered monetary instruments and are international in scope.

For their part, Canadian partners recognize that they are not as fully equipped, nor organized, as they could be to respond more effectively to the problem of MMF in Canada. They fully appreciate the importance of removing the profit from MMF activities and balancing out the risk-reward ratio by instituting a series of measures designed to disrupt, dismantle, and neutralize Canadian-based operators involved in these activities.

Partnerships and task forces have been cooperative in some instances but do not actively coordinate investigation to target MMF activities and trends at a national level. All of the cases examined involved Canadian suspects targeting U.S. consumers and required cross-border coordination and cooperation between law enforcement in Canada and the U.S.

The strategy developed by the NMMWG is currently reshaping the Canadian response and the current work being completed on the various pillars will expand the knowledge base of all stakeholders.

Investigations undertaken by the partnerships and task forces identify that MMF is organized and that MMF operators can be associated to multiple criminal enterprises, including but not limited to money laundering, drug operations, counterfeiting, and weapons. Investigations have also revealed that criminals involved in MMF operations were linked to gang activity and protection rackets. It is strongly suspected that proceeds from MMF operations were used to finance the other criminal activities.

Some MMF operations have the capabilities to infiltrate the legitimate economy and to use legitimate businesses to facilitate the communication components and proceeds components of the schemes.

MMF is a crime that requires a cooperative response from law enforcement, regulatory agencies, government and private sector. Existing task forces and partnerships are having great success in investigating MMF but they are limited by their resources.

APPENDICES

APPENDIX — A

Overall 2006 Top 12 Schemes reported by Canadians

(Current as of March 14, 2007)

In attempting to come up with a more accurate list of top Canadian reported MMF complaints, a comparative analysis was undertaken by a subject matter expert (SME) group, of Top 10 MMF scam lists from PhoneBusters, RECOL and the Competition Bureau while considering lists from the Better Business Bureau and Consumer Sentinel. This group also identified working definitions that could be used by various stakeholders in Canada.

1-Prize/Lottery/Sweepstakes: any false, deceptive or misleading solicitation advising victims they have won or have a chance to win something but are required to purchase something first or pay an advance fee, such as taxes to receive the prize. (e.g. You've won a car! But, first you must pay a fee.)

2-Work At Home / Job Opportunities: any false, deceptive or misleading solicitation offering employment and requesting an advance fee to secure the job or obtain the materials to perform the job or any job offer involving money transfer or wiring funds related to cashing monetary instruments.

3-Foreign Money Offer: traditionally referred to as Nigerian fraud, 419 fraud or West African fraud, these solicitations commonly offer or request assistance in the transfer of a large sum of money from international countries to the victim's country. Victim must pay a fee up front for various reasons (tax / processing fee / anti-terrorist certificate / black money washing fee / etc.) before the "fortune" can be released. However, the fortune is fictitious and the victim never receives what was promised.

4-Loan Scam: any false, deceptive or misleading solicitation involving the advertisement in a publication such as newspaper classified ads, magazines or through online ads and websites, offering a loan regardless of consumer's credit history. A victim responds to the ad and is required to send an advance fee in order to receive the loan, but never receives it.

5-Overpayment Scam: (Sale of Merchandise by Complainant): any incident involving a consumer selling merchandise or a service and receiving a payment in the form of a counterfeit or altered monetary instrument (e.g. cheque, money order) from the suspect for more than the asking price. The vendor is then directed to cash the cheque and send the extra amount back (send it to the shipping agent). Ultimately, the consumer is responsible to pay back any funds sent after cashing the cheque and may lose the sold merchandise if it has been shipped.

6-Business Directory: involves the sale of specialized directories (hard copies, CD-ROM or Internet) to businesses and non-profit organizations using misleading representations and deceptive sales techniques, such as the "assumed sale". Under the assumed sale technique, telemarketers target organizations with scripts, rebuttals, collection services and verification processes that are designed to "close" a sale that has never taken place. Various scenarios are used to lead targeted organizations into believing that contract obligations exist between them and the deceptive telemarketing operations.

7-Office Supplies: any false, deceptive or misleading solicitation involving assumed sales tactics in which the suspect company misrepresents itself as the victim's usual supplier, often by confirming their address and by pretending to offer the product at a discounted price or on a free trial basis. The victim receives an invoice and sees that the product is overpriced and not from their usual supplier. The suspect will often refuse return of the shipment, or will demand a re-stocking fee. The victim receives the supplies and begins using the product. After using a portion or the entire product, the victim receives an invoice for the product for more money than they would have to pay their usual supplier.

8-Vacation/Travel: any false, deceptive or misleading solicitation in which an advance fee is required to secure or hold a vacation. This commonly involves a failure to disclose material information, through the guise of receiving a free gift or reward, designed to convince victims to attend sales presentations where they are subjected to high-pressure sales and/or misleading representations.

9-Deceptive Health-Related Products or Services: Any false, deceptive or misleading promotion of, or solicitation regarding, health products or services relating to cures or treatments where the claims cannot be substantiated, or where consumers receive bogus products or treatments that do not work as advertised, if at all. Examples include product/service claims in the following areas of health cures or treatments: cancer, anti-aging and mental health.

10-Merchandise Purchased: (not received/not what it is supposed to be): The victim receives a bill or pays for merchandise that was not ordered or received. This commonly involves buying products over the Internet, or through a catalogue or by mail order, and never receiving the items.

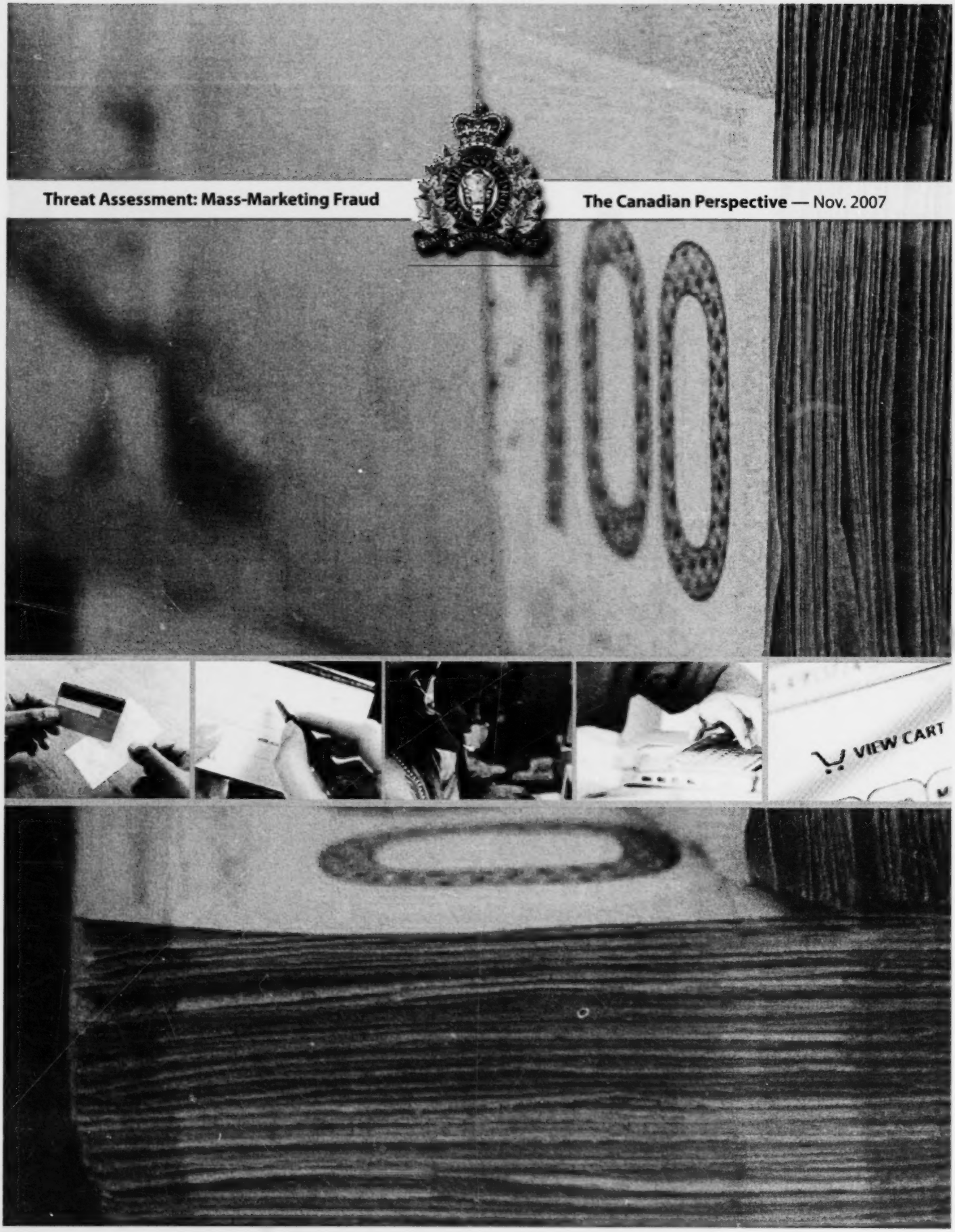
11- Credit Card: any false, deceptive or misleading solicitation in which consumers are offered and pay for a credit card up front but never receive the card.

12- Investment: any solicitation for investments into false, deceptive or misleading investment opportunities, often offering higher than normal or true monetary returns in which consumers lose most or all of their money that is supposedly invested.

APPENDIX — B

CANADIANS TARGETING OTHER COUNTRIES IN 2006
Complaints Involving Reported Dollar Loss Made to the Canadian Anti-fraud Call Centre from Foreign Victims

	TELEMARKETING (PHONE)			MAIL / PRINT			INTERNET / EMAIL		
Complaintant's	Attempts	Victim	Dollar Loss Reported	Attempts	Victims	Dollar Loss Reported	Attempts	Victims	Dollar Loss Reported
United States	6443	5165	$18,858,536.08	1893	566	$1,683,746.99	206	437	$875,116.05
Australia	0	1	$168,467.00	4	0	$0.00	0	2	$40.94
United Kingdom	8	18	$154,847.03	6	1	$50.00	0	5	$413.86
Germany	0	1	$64,000.00	0	0	$0.00	0	2	$5,662.63
France	0	2	$32,485.00	0	0	$0.00	1	0	$0.00
Sweden	0	1	$20,278.00	0	0	$0.00	0	0	$0.00
Thailand	0	1	$16,879.19	0	0	$0.00	0	0	$0.00
Puerto Rico	0	1	$2,839.00	0	0	$0.00	0	0	$0.00
India	0	1	$157.84	0	0	$0.00	0	0	$0.00
Austria	0	0	$0.00	0	1	$5,530.55	0	0	$0.00
Guatemala	0	0	$0.00	0	1	$189.00	0	0	$0.00
Netherlands	0	0	$0.00	0	0	$0.00	0	1	$126.00
Japan	0	0	$0.00	0	0	$0.00	0	1	$162.50



Threat Assessment: Mass-Marketing Fraud

The Canadian Perspective — Nov. 2007